UNIVERSIDAD NACIONAL DE PIURA

FACULTAD DE INGENIERÍA INDUSTRIAL

ESCUELA PROFESIONAL DE INGENIERÍA INFORMÁTICA

TESIS

APLICACIÓN DE LA METODOLOGÍA MAGERIT PARA LA ELABORACIÓN DE UN PLAN DE MEJORA DE LA SEGURIDAD DE LOS ACTIVOS DE INFORMACIÓN DE LA ZONA ESPECIAL DE DESARROLLO – ZED PAITA

PRESENTADO POR:

Briceño Huaygua, Cristhian Abijail

TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO INFORMÁTICO

LÍNEA DE INVESTIGACIÓN:

INFORMÁTICA, ELECTRÓNICA Y TELECOMUNICACIONES

SUB LÍNEA DE INVESTIGACIÓN:

COMPUTACIÓN

PIURA, PERÚ

2019

UNIVERSIDAD NACIONAL DE PIURA

FACULTAD DE INGENIERÍA INDUSTRIAL

ESCUELA PROFESIONAL DE INGENIERÍA INFORMÁTICA

TESIS

APLICACIÓN DE LA METODOLOGÍA MAGERIT PARA LA ELABORACIÓN DE UN PLAN DE MEJORA DE LA SEGURIDAD DE LOS ACTIVOS DE INFORMACIÓN DE LA ZONA ESPECIAL DE DESARROLLO – ZED PAITA

BRICEÑO HUAYGUA, CRISTHIAN ABIJAIL
TESISTA

DR. RIGO FELIX REQUENA FLORES
ASESOR

DR. MOISES DAVID SAAVEDRA ARANGO
CO - ASESOR

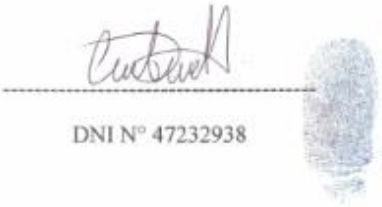
DECLARACIÓN JURADA DE ORIGINALIDAD DE LA TESIS

Yo, **CRISTHIAN ABIJAIL, BRICEÑO HUAYGA,** identificado con DNI N° 47232938, Bachiller de la Facultad de Ingeniería Industrial, Escuela Profesional de Ingeniería Informática y domiciliado en A.H Marco Jara D-36 Etapa I, en la provincia de Paita, departamento de Piura, Celular: 937503155, Email: brice180@gmail.com.

"APLICACIÓN DE LA METODOLOGÍA MAGERIT PARA LA ELABORACIÓN DE UN PLAN DE MEJORA DE LA SEGURIDAD DE LOS ACTIVOS DE INFORMACIÓN DE LA ZONA ESPECIAL DE DESARROLLO – ZED PAITA"

DECLARO BAJO JURAMENTO, que la tesis que presento es original e inédita, no siendo copia parcial ni total de una tesis desarrollada, y/o realizada en el Perú o en el Extranjero, en caso contrario de resultar falsa la información que proporciono, me sujeto a los alcances de lo establecido en el Art. N° 411 del código Penal concordante con el Art. 32° de la ley 27444, Ley del Procedimiento Administrativo General y las Normas Legales de Protección a los Derechos de Autor. En fe de lo cual firmo la presente.

Piura, 31 de julio del 2019



DNI N° 47232938

Artículo 411.- El que, en un procedimiento administrativo, hace una falsa declaración en relación con hechos o circunstancias que le corresponde probar, violando la presunción de veracidad establecida por la ley, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años.

Art. 4 Inciso 4.12 del Reglamento del Registro Nacional de Trabajos de Investigación para optar grados académicos y títulos profesionales – RENATI Resolución de Consejo Directivo N° 033-2016-SUNEDU/CD

UNIVERSIDAD NACIONAL DE PIURA
FACULTAD DE INGENIERÍA INDUSTRIAL
DECANATO

ACTA DE EVALUACIÓN Y SUSTENTACIÓN DE TESIS

Expediente N° 1451 / 2017

Los miembros del Jurado Calificador Ad-Hoc de la Sustentación de Tesis nombrado con Resolución N° **488-CF-FII-UNP-17** de fecha 28/08/2017 que suscriben, se reunieron en acto público en la sala de exposiciones de la Facultad de Ingeniería Industrial de la Universidad Nacional de Piura, el día **27 de Diciembre del 2019** a las **10:00 am**, para evaluar la defensa de la Tesis titulada **"APLICACIÓN DE LA METODOLOGÍA MAGERIT PARA LA ELABORACIÓN DE UN PLAN DE MEJORA DE LA SEGURIDAD DE LOS ACTIVOS DE INFORMACIÓN DE LA ZONA ESPECIAL DE DESARROLLO-ZED PAITA"**, presentada por el Bachiller **CRISTHIAN ABIJAIL BRICEÑO HUAYGUA** y asesorado por el **Dr. RIGO FÉLIX REQUENA FLORES** y co-asesorado por el **Dr. MOISÉS DAVID SAAVEDRA ARANGO**.

Después de haber calificado el Informe Final de la Tesis, escuchada la sustentación y las respuestas a las preguntas formuladas por el Jurado, se le declara ....APROBADA.... para optar el Título de **INGENIERO INFORMÁTICO** con el puntaje de ..75... que corresponde al calificativo de ....MUY BUENO....

Calificación \ Jurado	Presidente	Secretario	Vocal	Puntaje Promedio
Documento (Max 60 puntos)	40	40	40	40
Sustentación (Max 40 puntos)	35	35	35	35
PUNTAJE TOTAL				75

En consecuencia, el sustentante queda en condición de recibir el Título Profesional que se indica, conferido por el Consejo Universitario de la Universidad Nacional de Piura de conformidad con las Normas Estatutarias y la Ley Universitaria en vigencia.

FACULTAD DE INGENIERÍA INDUSTRIAL Dirección de Investigación UNP

Ciudad Universitaria, 27 de Diciembre del 2019

Dr. VÍCTOR HUGO RAMÍREZ ORDINOLA	Dr. FRANCISCO JAVIER CRUZ VÍLCHEZ	Ing. NÉSTOR MANUEL CASTILLO BURGOS
PRESIDENTE	**SECRETARIO**	**VOCAL**

UNIVERSIDAD NACIONAL DE PIURA

FACULTAD DE INGENIERÍA INDUSTRIAL

ESCUELA PROFESIONAL DE INGENIERÍA INFORMÁTICA

INFORME FINAL DE TESIS

"APLICACIÓN DE LA METODOLOGÍA MAGERIT PARA LA ELABORACIÓN DE UN PLAN DE MEJORA DE LA SEGURIDAD DE LOS ACTIVOS DE INFORMACIÓN DE LA ZONA ESPECIAL DE DESARROLLO – ZED PAITA"

JURADO AD HOC

DR. VÍCTOR HUGO RAMÍREZ ORDINOLA
PRESIDENTE

DR. FRANCISCO JAVIER CRUZ VÍLCHEZ
VOCAL

ING. NÉSTOR MANUEL CASTILLO BURGOS
SECRETARIO

DEDICATORIA

A Dios, mi luz y guía en el camino de la vida, quien cuida mis pasos en todo tiempo.

A mis padres y hermanos, quienes son el motivo para seguir conquistando sueños y cumpliendo metas.

A mi futura esposa, con quien compartiré mis días hasta que la muerte nos separe.

AGRADECIMIENTO

Agradezco a Dios por darme la bendición de tener excelentes padres que se preocuparon por darme una mejor educación

A mis padres que dieron todo su esfuerzo para hacerme una mejor persona, por inculcarme buenos valores y por su apoyo moral y económico para poder cumplir esta meta satisfactoriamente.

A todas las personas involucradas en este proyecto.

RESUMEN

En los últimos años fuimos testigos de grandes fugas de información, por ejemplo, el caso de los documentos filtrados por WikiLeaks o los famosos Panamá Papers, esto pone en evidencia las falencias que existen en las empresas y la poco conciencia de seguridad de la información, no tomando en cuento de los riesgos y de las amenazas a los que están expuesto todos los activos de una empresa, en este caso la información.

En el presente trabajo se describen los riesgos y las amenazas a los que están expuestos los activos de una empresa en particular, lo cual no es tan distante a la realidad de todas las empresas de la región y de nuestro país. Es de vital importancia que las Instituciones tomen conciencia de los impactos que generarían la materialización de alguna amenaza y que el modelo de negocio de la Institución se vea afectados directa o indirectamente, como los casos que se mencionó anteriormente.

El presente trabajo sienta las bases para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), ya que abarca los pasos iniciales para la implementación del mencionado Sistema, porque ayuda a conocer el estado actual en el que se encuentra la Institución, y de esta manera se integre a los procesos y la estructura de gestión general.

Finalmente, la aportación de la presente investigación es dar a conocer a la empresa, su situación actual y proponer un Plan de Mejora para que a través de Políticas de Seguridad se minimice el riesgo y el impacto a los que están expuestos todos los activos de la empresa, este Plan de Mejora se redactó en acorde al cumplimiento de la Norma Técnica Peruana NTP-ISO/IEC 27001:2014.

Palabras Claves: Riesgo, Amenaza, Activo, Impacto, Plan de Mejora, SGSI.

ABSTRACT

In recent years we witnessed major information leaks, for example, the case of documents leaked by WikiLeaks or the famous Panama Papers, this highlights the shortcomings that exist in companies and the little awareness of information security, not taking into account the risks and threats to which are exposed all the assets of a company, in this case information.

This paper describes the risks and threats to which the assets of a particular company are exposed, which is not so distant from the reality of all companies in the region and in our country. It is of vital importance that the Institutions become aware of the impacts that would be generated by the materialization of any threat and that the business model of the Institution is directly or indirectly affected, as in the cases mentioned above.

This paper lays the foundations for the implementation of an Information Security Management System (ISMS), since it covers the initial steps for the implementation of the mentioned System, because it helps to know the current state in which the Institution is, and in this way it is integrated to the processes and the general management structure.

Finally, the contribution of this research is to make the company aware of its current situation and to propose an Improvement Plan so that, through Security Policies, the risk and impact to which all the company's assets are exposed are minimised. This Improvement Plan was drawn up in accordance with compliance with the Peruvian Technical Standard NTP-ISO/IEC 27001:2014.

Keywords: Risk, Threat, Asset, Impact, Improvement Plan, ISMS.

ÍNDICE GENERAL

ÍNDICE TABLAS

ÍNDICE GRÁFICOS

INTRODUCCIÓN

Desde hace ya algunos años la información se considera uno de los activos más valiosos de una compañía, los costos derivados de la pérdida de seguridad de la información no son sólo costos económicos directos, sino que también afectan a la imagen de la empresa, por lo que cada vez más, la seguridad de la información forma parte de los objetivos de las organizaciones y, sin embargo, a pesar de esa concienciación generalizada, muchas entidades no se enfrentan a este aspecto con la profundidad con la que debiera tratarse.

Hoy en día los activos de información han pasado a formar parte de la actividad cotidiana de organizaciones e individuos; los equipos de cómputo almacenan información, la procesan y la transmiten a través de redes y canales de comunicación, abriendo nuevas posibilidades y facilidades a los usuarios, pero se deben considerar nuevos paradigmas en estos modelos tecnológicos y tener muy claro que no existen sistemas cien por ciento seguros, porque el costo de la seguridad total es muy alto (aunque en la realidad no es alcanzable idealmente), y las organizaciones no están preparadas para hacer este tipo de inversión.

La Zona Especial de Desarrollo Paita, en adelante ZED PAITA, es una entidad en crecimiento que debe involucrar dentro de sus procesos buenas prácticas encaminadas a la protección de la información; razón por la cual es necesario el desarrollo de un análisis de los riesgos a los que están expuestos los activos de información y conocer los mecanismos que puedan minimizar la materialización de las amenazas, así de esta manera poder elaborar un plan de mejora de seguridad de los activos de información.

CAPÍTULO I

EL PROBLEMA DE INVESTIGACIÓN

CAPÍTULO I.- EL PROBLEMA DE INVESTIGACIÓN

1.1. Descripción de la realidad problemática

Actualmente la información es uno de los activos más importantes de una organización, su valor es relativamente alto en comparación a otros activos existentes, esta se ha convertido en la base fundamental para el logro de los objetivos y sobrevivencia de las mismas, por ende, las organizaciones están propensas a una serie de riesgos mientras no se garantice un entorno totalmente seguro para su información.

ZED PAITA, es un organismo público descentralizado adscrito al Gobierno Regional de Piura, que tiene personería jurídica de derecho público, con autonomía administrativa, técnica, económica, financiera y operativa, sujeta a la supervisión y regulación de su funcionamiento por parte del Ministerio de Comercio Exterior y Turismo (MINCETUR), quien propone las políticas. El Gobierno Regional supervisa la administración, la promoción y desarrollo del mismo.

Su propósito es proporcionar y difundir el conocimiento y la importancia de la ZED PAITA, como plataforma logística y por lo tanto la existencia de la posibilidad para todas las empresas de tener oportunidad de obtener ahorros considerables en su gestión y elevar sus niveles de competitividad, configurando un clima empresarial favorable, así como promover, desarrollar e impulsar el desarrollo de las distintas actividades de producción y en especial las de agro-exportación y agroindustrial, aprovechando su posición geoestratégica dentro de la región norte del país y su cercanía al puerto de Paita – Perú.

A medida que la ZED PAITA ha ido madurando como empresa, no se ha ido tomando en cuenta que los activos de información están expuestos a riesgos y amenazas, que podrían comprometer la integridad, confidencialidad y disponibilidad de la información.

Actualmente existen procedimientos creados por iniciativa y experiencia de los miembros del equipo de la Oficina de Tecnologías de la Información; por ejemplo, se controla el acceso a la entidad de equipos informáticos como laptops, memorias USB, y otros dispositivos electrónicos, pero no existe una política de uso de claves de usuario para el acceso a los Sistemas de Información, en lo que respecta a los servidores se realiza el cambio de claves de acceso a criterio del personal responsable de cada uno de ellos sin una periodicidad y política definida.

La entidad ZED PAITA ya ha sufrido algunos inconvenientes dentro del manejo de la información, esto, debido a que ha ido creciendo y no se ha tomado conciencia de la importancia de asegurar la información existente; lo que aumenta las probabilidades que en un futuro cercano vuelvan a ocurrir incidencias relacionadas con la seguridad de su información.

Conforme al crecimiento que experimenta la ZED PAITA es necesario adoptar y crear procedimientos que regulen las buenas prácticas en cada una de las transacciones, procesos y recursos relacionados con la información. Para tal fin se debe implementar un plan de mejora que regule todos estos procedimientos, además que este será una base fundamental para que más adelante se pueda implementar un Sistema de Gestión de Seguridad de la Información (SGSI) certificado por entidades especializadas en el rubro.

De no integrar dentro de sus sistemas, buenas prácticas y recomendaciones de seguridad informática, muy seguramente en un futuro cercano la ZED PAITA podría ser víctima de delitos informáticos que obstaculicen su normal funcionamiento, además de generar una mala imagen dentro del mundo empresarial.

1.2. Formulación del Problema

¿Cómo elaborar un plan de mejora de la seguridad de los activos de información en la Zona Especial de Desarrollo - ZED PAITA?

1.3. Justificación, Importancia y Beneficiarios de la Investigación

La entidad ZED PAITA debe tomar conciencia de la necesidad de alinear sus objetivos institucionales, asegurando el flujo de información, optimizando recursos y garantizando la Confidencialidad, Disponibilidad e Integridad de la misma. Este es uno de los retos que debe asumir la entidad para estar acorde a los modelos y estándares nacionales e internacionales, para ello es necesario empezar con la ejecución del análisis de riesgos de la seguridad de la información que en un futuro será la base para implementar el Sistema de Gestión de Seguridad de la Información (SGSI), que permitirá mantener un modelo de negocio estable, logrando un valor agregado y posicionamiento a nivel regional.

La importancia de tener un plan de mejora actualizado en la entidad ZED-PAITA, es con el fin de garantizar mayor efectividad y eficiencia dentro de cada uno de sus procesos; teniendo en cuenta que al conocer las fortalezas y debilidades se mejora el control y administración de recursos tecnológicos acorde a las normas nacionales e internacionales que buscan proporcionar mecanismos y herramientas para adoptar buenas prácticas de seguridad y que de esta forma se logren los objetivos institucionales.

Para lograr el cumplimiento del objetivo planteado, se pretende saber cómo la aplicación de la metodología MAGERIT logrará definir correctamente el proceso para poder verificar y obtener información actualizada de los riegos a que están expuestos los activos de información, las amenazas que los rodean, así como las salvaguardas o procesos de mitigación, para de esta manera llegar a definir un plan de mejora actualizado de acorde a las necesidades que la institución.

Los beneficiarios tras desarrollar este trabajo de investigación son:

- **Beneficiarios directos**: La Zona Especial de Desarrollo Paita – ZED PAITA.

- **Beneficiarios indirectos**: Empresas usuarias que desarrollan sus actividades dentro de los límites territoriales de la ZED PAITA.

1.4. Objetivos de la Investigación

1.4.1. Objetivo General:

Aplicar la metodología MAGERIT para elaborar un Plan de Mejora de la Seguridad en los activos de información de la ZED PAITA.

1.4.2. Objetivos Específicos:

- Identificar y valorar los activos de información relevantes para la entidad ZED PAITA.
- Determinar y analizar a qué amenazas están expuestos estos activos de información de la ZED PAITA
- Proponer salvaguardas para minimizar los riesgos que pueden materializarse tras las amenazas a los que están expuestos los activos de la ZED PAITA
- Diseñar un modelo de seguridad basado en la Norma Técnica Peruana NTP-ISO/IEC 27001 – 2014

1.5. Hipótesis:

1.5.1. Hipótesis General:

La aplicación de la metodología MAGERIT permitirá elaborar un Plan de Mejora de la Seguridad de los activos de información en la Zona Especial de Desarrollo – ZED PAITA.

1.6. Identificación y Operacionalización de Variables

- **Variable Independiente**

En el cuadro se hace referencia a la variable independiente, su definición, indicadores y los instrumentos de medición que se utilizarán para el desarrollo de la presente investigación.

Variable	**Definición**	**Dimensión**	**Indicadores**
Aplicación metodología MAGERIT	Aplicación de la metodología MAGERIT, en la entidad ZED Paita.	Disponibilidad Integridad Confidencialidad Autenticidad	Tipo de activo
			Valoración estimada
		Amenaza	Tipo de amenaza
			Probabilidad de ocurrencia de la amenaza
			Impacto
		Salvaguarda	Tipo de salvaguarda
			Valoración estimada

Tabla 01: Descripción de la variable independiente
Fuente: Elaboración propia.

- **Variable Dependiente**

Plan de Mejora de la Seguridad.

1.7. Metodología: Métodos y Materiales

1.7.1. Tipo de Investigación:

Se considerará una investigación aplicada. Este tipo de investigación está vinculada a la aplicación de una metodología en un caso particular como es el Análisis de Riesgos Informáticos en la Entidad ZED PAITA, permitiendo la búsqueda de una posible solución a los problemas conocidos o que aún se desconocen de acuerdo a los riesgos informáticos que se pueden presentar o que se están presentando en la Entidad.

Además, se considerará como una investigación descriptiva, debido a que se observará el comportamiento de los activos de información, realizando un análisis y proponiendo mecanismos de control sobre los riesgos asociados a ellos, sin influir en los procesos actuales, dejando en manos de la empresa si desea o no desea implementarlos.

1.7.2. Diseño de Investigación:

El diseño de Investigación será de tipo no experimental ya que manipularemos la variable independiente (Metodología MAGERIT) para poder analizar y gestionar el comportamiento de la variable dependiente que en este caso sería verificar el nivel de seguridad que alcanzarían los activos de información si se implementara un Plan de Mejora.

1.7.3. Procedimientos, Técnicas e Instrumentos de recolección de información:

1.7.3.1. Procedimientos

Se utilizará la metodología MAGERIT para el análisis y gestión de los riesgos asociados a los activos de la información. La información obtenida será para obtener los

datos necesarios para diseñar un Plan de Mejora adecuados a la Institución. Estos serán procesados de la mejor manera posible para demostrar los resultados de la misma.

1.7.3.2. Técnicas

- ***Observación directa***

Esta técnica se utilizará para captar los hechos que acontecen en la entidad para obtener los datos más próximos que ocurren en la realidad.

- ***Entrevistas***

Por medio de esta técnica, se recaudará la información proveniente de los diferentes usuarios con el fin de realizar el análisis y gestión de los riesgos asociados a los activos de información el cual nos permitirá obtener información empírica necesaria para la investigación.

1.7.3.3. Instrumentos de recolección y procesamiento de datos

Se recolectarán los datos a través de la observación directa, y con entrevistas al Jefe del área de Informática, dándoles un valor a cada activo de información de acuerdo con una escala predefinida en la Metodología MAGERIT.

1.8. Cobertura de Estudio:

1.8.1. Población:

La presente investigación se realizará en la entidad ZED PAITA, en cada una de las oficinas que laboran actualmente el personal, siendo un total de 25 usuarios.

1.8.2. Muestra:

Debido a que la población es pequeña, se trabajó con el total de la población y no se especificó la muestra.

1.9. Técnicas de procesamiento, análisis e interpretación de datos.

El procesamiento de datos será a través del Software PILAR en su Versión 6.2.6 para el análisis de riesgos bajo un enfoque cualitativo y la realización de análisis de impacto en el ámbito de la continuidad de negocio.

CAPÍTULO II

MARCO TEÓRICO

CAPITULO II - MARCO TEÓRICO:

2.1. Marco Institucional

2.1.1. Nombre de la Empresa

Zona Especial de Desarrollo Paita – ZED PAITA.

2.1.2. Descripción de la Empresa

ZEDPAITA, es un organismo público descentralizado adscrito al Gobierno Regional de Piura, que tiene personería jurídica de derecho público, con autonomía administrativa, técnica, económica, financiera y operativa, sujeta a la supervisión y regulación de su funcionamiento por parte del MINCETUR quien propone las políticas. El Gobierno Regional supervisa la administración, la promoción y desarrollo del mismo.

Su propósito es proporcionar y difundir el conocimiento y la importancia de la ZED PAITA, como plataforma logística y por lo tanto la existencia de la posibilidad para todas las empresas de tener oportunidad de obtener ahorros considerables en su gestión y elevar sus niveles de competitividad, configurando un clima empresarial favorable, así como promover, desarrollar e impulsar el desarrollo de las distintas actividades de producción y en especial las de agro-exportación y agroindustrial, aprovechando su posición geoestratégica dentro de la región norte del país y su cercanía al puerto de Paita – Perú.

La Zona Especial de Desarrollo: "ZED PAITA", constituye un área geográfica debidamente delimitada, que tiene la naturaleza de "zona primaria aduanera".

2.1.2.1. Histórica Institucional

1996 *Un año de especial significación:* La historia comienza hace 20 años, exactamente un domingo 27 de octubre de 1996, con la entrada en vigencia del Decreto Legislativo N° 864; norma que crea el Centro de Exportación, Transformación, Industrias, Comercialización y Servicios de Paita – CETICOS PAITA, destinado a promover la inversión privada en el norte del país.

2001 *Más dinámicos con mayores beneficios*: Con la entrada en vigencia del Decreto Supremo Nº 008-2001-ITINCI se estableció que las actividades de transformación realizadas por los usuarios podían gozar de los mismos beneficios y condiciones aplicables o exigibles a las actividades de manufactura.

2005 *Mejores decisiones, mejores resultados*: Con la finalidad de continuar contribuyendo con el desarrollo de la zona norte del país, se nos otorgó autonomía administrativa, técnica, económica, financiera y operativa con personería jurídica de derecho público, a través de la Ley 28569.

2007 *Supervisión sostenible con el tiempo*: Con la Ley 29014, los gobiernos regionales pasan a supervisar y regular el funcionamiento de los CETICOS tanto en la administración, promoción y el desarrollo de éstos, respetando nuestra autonomía.

2009 *Continuidad para el desarrollo*: Con la finalidad de establecer un principio de equidad jurídica y no discriminatoria, respecto a Zofratacna (Zona Franca de Tacna), en el 2009 con la entrada en vigencia de la Ley 29479 se prorroga el plazo de las exoneraciones hasta el 2022 de las empresas usuarias instaladas y de las mercancías que permanezcan en los CETICOS.

2011 *Fortalecemos nuestros beneficios*: Con la entrada en vigencia de la Ley N° 29710, el desarrollo de las actividades autorizadas en los CETICOS queda exonerada de impuestos, así como de todo tributo, creado o por crearse, incluso de los que requieran de norma exoneraría expresa, excepto las aportaciones a EsSalud y las tasas.

2016 *Nuevo nombre para nuevos horizontes*: El 03 de junio de este año, se aprobó la Ley 30446, la cual cambia de denominación de los CETICOS por el de ZED (Zona Especial de Desarrollo) y, amplía el plazo de vigencia de los beneficios, exoneraciones y permanencia de mercancías hasta el 31 de diciembre de 2042.

2.1.2.2. Misión

ZED PAITA, es una zona primaria aduanera de tratamiento especial, promueve polos de desarrollo a través de la inversión privada con el fin de incrementar el empleo, el consumo de productos y servicios en su ámbito de influencia, y las exportaciones para fortalecer la economía regional. También promueve y brinda servicios de calidad a sus usuarios para que mejoren su competitividad empresarial.

2.1.2.3. Visión

ZED PAITA, progresivamente hasta el 2042 se convertirá en zona fundamental del desarrollo económico regional y del país, y, con la puesta en marcha de iniciativas innovadoras y competitivas, promoverá la inversión privada en el 100% de su área habilitada actual.

2.1.2.4. Estructura Organizacional

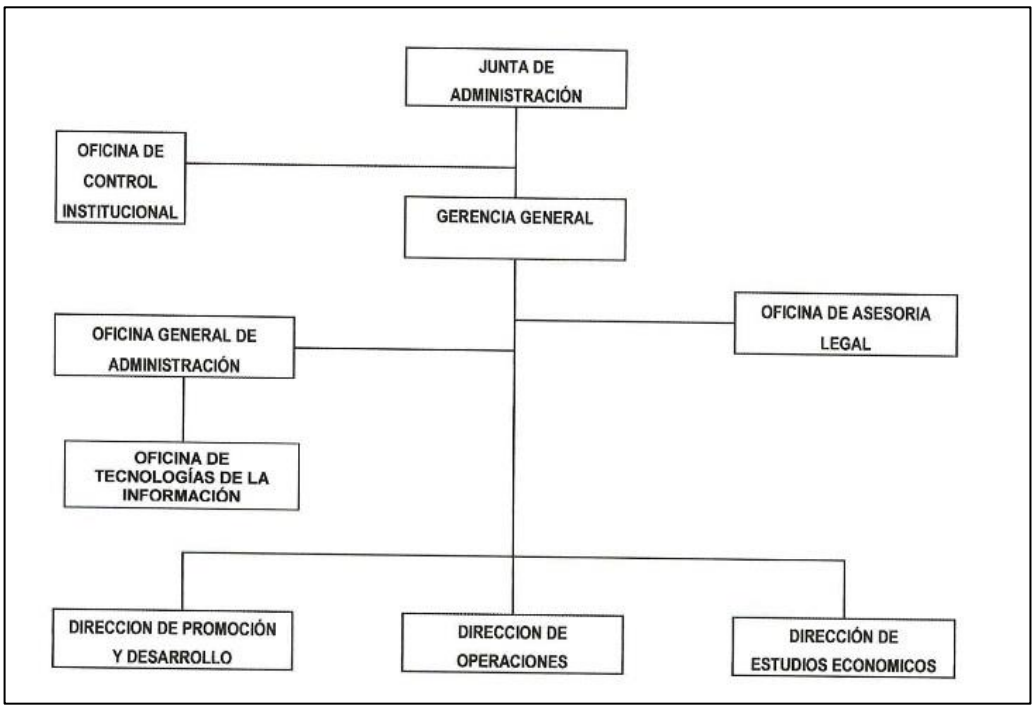


Gráfico 01: Organigrama de la Institución.

Fuente: ZED PAITA

2.2. Marco Teórico

2.2.1. Auditoría Informática

"Auditoría Informática es el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informático salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos" (Piattini, 2001).

Según Piattini, la Auditoría Informática consiste en realizar una evaluación exhausta de cómo está funcionando el sistema informático y conocer su rendimiento ante los diferentes procesos que existen dentro de la empresa.

"Es la revisión técnica, especializada y exhaustiva que se realiza a los sistemas computacionales, software e información utilizados en una empresa, sean individuales, compartidos y/o de redes, así como a sus instalaciones, telecomunicaciones, mobiliario, equipos periféricos y demás componentes." (Muñoz, 2002).

Según Carlos Muñoz en su concepto de Auditoría Informática, indica que no es más que una revisión técnica minuciosa a los diferentes sistemas computacionales utilizados en la empresa para así conocer su respectivo desempeño.

"La Auditoría Informática es un examen metódico del servicio informático en particular, realizado de una forma puntual y de modo discontinuo, a instancias de la Dirección, con la intención de ayudar a mejorar conceptos como la seguridad, la eficiencia, y la rentabilidad del servicio, o del sistema, que resultan auditados" (Rivas, 1988).

Al leer los conceptos mencionados por los autores anteriores se puede decir que la Auditoría Informática es un proceso donde profesionales capacitados acumulan, agrupan y evalúan pruebas para determinar si un sistema de información mantiene la integridad de los datos, cumple con los fines de la empresa, y desempeña bien las leyes implantadas en la organización.

2.2.2. Riesgo Informático

Para entender el significado de lo que es un riesgo, se exponen las siguientes definiciones:

Según Fernando Izquierdo Duarte: "El Riesgo es un incidente o situación, que ocurre en un sitio concreto durante un intervalo de tiempo determinado, con consecuencias positivas o negativas que podrían afectar el cumplimiento de los objetivos" (Izquierdo, 2005).

Según (Pinilla, 1997) “El riesgo es una condición del mundo real en el cual hay una exposición a la adversidad, conformada por una combinación de circunstancias del entorno, donde hay posibilidades de pérdidas”

Según Martín Vilches Troncoso: “El riesgo es cualquier variable importante de incertidumbre que interfiera con el logro de los objetivos y estrategias del negocio. Es decir, es la posibilidad de la ocurrencia de un hecho o suceso no deseado o la no ocurrencia de uno deseado.”

En consiguiente, el proceso de análisis de riesgos debe ser el más importante de la gestión de la seguridad de la información de una organización, de aquí parte la gestión de los riesgos, que es en última instancia con la que se decide tomar la decisión de eliminarlos, ignorarlos, mitigarlos y controlarlos, es decir aplicar la gestión de riesgos basados en la compleja tarea de determinar, analizar, evaluar y clasificar los activos de información más importantes según la criticidad de los mismos.

2.2.3. Riesgos en el Manejo de la Información

“El manejo de riesgos dentro de la seguridad en la información implica:

Evitar: No se permite ningún tipo de exposición. Esto se logra simplemente con no comprometerse a realizar la acción que origine el riesgo.

Reducir: Cuando el riesgo no puede evitarse por tener varias dificultades de tipo operacional, la alternativa puede ser su reducción hasta el nivel más bajo posible. Esta opción es la más económica y sencilla.

Retener, Asumir o Aceptar el riesgo: Aceptar las consecuencias de la ocurrencia del evento. Puede ser voluntaria, que se caracteriza por el reconocimiento de la existencia del riesgo o también puede ser involuntaria la cual se da cuando el riesgo es retenido inconscientemente.

Transferir: Es buscar un respaldo y compartir el riego con otros controles o entidades.” (Hernandez, 2009).

En resumen (Hernandez, 2009) menciona que los riesgos en el manejo de la información se dan de diferente manera hasta el punto en el que se puede utilizar técnicas como es el evitar a no realizar tal acción de la que puede surgir el riesgo; como también reducir el conflicto al nivel más bajo si ya se generó el riesgo.

2.2.4. Metodologías de Análisis de Riesgo.

Para mitigar los riesgos en el manejo de la información existen diferentes Metodologías, entre algunas de ellas están:

2.2.4.1. CRAMM (Metodología De Análisis Y Gestión De Riesgos Desarrollada Por El CCTA inglés)

Es la metodología de Análisis de Riesgos desarrollado por el Centro de Informática y la Agencia Nacional de Telecomunicaciones (CCTA) del Gobierno del Reino Unido.

Puede definirse como una Metodología para el Análisis de Gestión de Riesgos que aplica sus conceptos de una manera formal, disciplinada y estructurada. Orientada a proteger la confidencialidad, integridad y disponibilidad de un sistema y de sus activos; que, aunque es considerada cuantitativa, utiliza evaluaciones cuantitativas y cualitativas, y por esto se considera mixta.

2.2.4.2. EBIOS (Metodología Francesa de Análisis y Gestión De Riesgos de Seguridad de Sistemas de Información).

Es un juego de guías más una herramienta de código libre gratuita, enfocada a gestores del riesgo de TI. Desarrollada en un principio por el gobierno francés.

La Metodología EBIOS consta de un ciclo de cinco fases como son: Fase 1: Análisis del contexto, estudiando cuales son las dependencias de los procesos del negocio respecto a los sistemas de información. Fase 2 y 3: Análisis de las necesidades de seguridad y de las amenazas, determinando los puntos de conflicto. Fase 4 y 5: Resolución del conflicto, estableciendo los objetivos de seguridad necesarios y suficientes, con pruebas de cumplimiento y dejando claros cuáles son los riesgos residuales.

2.2.4.3. OCTAVE (Metodología de Evaluación de Riesgos Desarrollada Por El SEI (Software Engineering Institute) de la Cornegie Mellon University)

Esta Metodología que es Evaluación de Amenazas Operacionalmente Críticas, de Activos y Vulnerabilidades, se implementa con la conformación de un equipo mixto, compuesto de personas de las áreas de negocio y de TI.

Esta configuración explica el hecho de que los funcionarios del negocio son los más indicados para identificar qué información es importante en los procesos y cómo se usa dicha información; por su parte el equipo de TI, es el que conoce la configuración de la infraestructura y las debilidades que pueden tener.

El proceso de evaluación contemplado por OCTAVE se divide en tres fases:

1.- Construcción de perfiles de amenazas basadas en activos.
2.- Identificación de vulnerabilidades en la infraestructura.
3.- Desarrollo de estrategias y planes de seguridad.

2.2.4.4. MAGERIT (Metodología de Análisis y Gestión de Riesgos para los Sistemas De Información)

Metodología de Análisis y Gestión de Riesgos elaborada por el Consejo Superior de Administración Electrónica, como respuesta a la percepción de que la Administración, y en general, toda la sociedad, dependen de forma creciente de las tecnologías de la información para el cumplimiento de su misión.

Siguiendo la terminología de la normativa ISO 31000, MAGERIT responde a lo que se denomina "Proceso de Gestión de los Riesgos", sección 4.4 ("Implementación de la Gestión de los Riesgos") dentro del "Marco de Gestión de Riesgos". En otras palabras, MAGERIT implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información.

2.3. Marco Conceptual

2.3.1. Seguridad Informática

"El conjunto de metodologías, prácticas y procedimientos que buscan proteger la información como activo valioso, con el fin de minimizar las amenazas y riesgos continuos a los que está expuesta, a efectos de asegurar la continuidad del negocio, minimizar los daños a la

organización y maximizar el retorno de inversiones y las oportunidades del negocio" (Hernandez, 2009).

Según Hernández, la Seguridad de la Información es muy importante en una empresa o individuo ya que con ello se llega a proteger toda información que sea importante y beneficiosa; y así evitar cualquier daño que pueda afectar a la Organización. "Se entiende por Seguridad de la Información a todas aquellas medidas preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información buscando mantener la confidencialidad, la autenticidad e integridad de la misma.

2.3.2. Características de un Sistema Seguro

Confidencialidad: Se refiere a que la información puede ser accedida únicamente por las personas que tienen autorización para hacerlo.

Es recomendable que las empresas otorguen a sus empleados de acuerdo con su función que desempeñan tener un determinado acceso a la información. Algunas empresas los contratos de emplea constan de cláusulas de confidencialidad donde no le es permitido a las personas revelar secretos profesionales, esto sería un mecanismo de seguridad que todas las empresas deberían usar para garantizar la seguridad de su información.

Integridad: Quiere decir que la información no haya sido borrada, copiada o alterada, durante el trayecto de origen a su destino.

La integridad es un factor fundamental al momento que recibimos un documento ya sea digitalmente o físicamente, nos brinda la confianza de estar seguros de que la información que se encuentra ahí no ha sufrido ninguna alteración.

Disponibilidad: Es el aseguramiento de que los usuarios autorizados tienen acceso a la información y sus activos asociados cuando lo requieran.

La disponibilidad de un sistema implica que tanto hardware y software se mantengan funcionando correctamente, eficientemente y sea capaz de recuperarse ante un caso de fallo.

2.3.3. Información

Es el conjunto de datos (numéricos, alfabéticos y alfanuméricos) procesados en forma significativa, ordenados y con una secuencia lógica sobre algún suceso o hecho de importancia. Con valor real para la toma de decisiones, a medida que tenemos más información, más fácil nos resulta tomar decisiones correctas. Esa es la función de la información: disminuir la incertidumbre o aumentar el conocimiento, aumentando la probabilidad de éxito. (Did, 2016)

2.3.3.1. Activos de Información

El activo esencial es la información que se maneja en los diferentes sistemas; es decir los datos, entorno a ello se identifican otros activos relevantes.

Los servicios que se pueden prestar a través de esos datos, y los servicios que se necesitan para gestionarlos. Las aplicaciones (Software) que permiten manejar los datos. Los equipos (Hardware) que permiten hospedar datos, aplicaciones y servicios. Los soportes de información, que son dispositivos de almacenamientos de datos. El equipamiento auxiliar que complementa el material informático. Las redes de comunicaciones que permiten intercambiar datos. Las instalaciones que acogen equipos informáticos y de

comunicaciones. Las personas que operan todos los elementos mencionados.

2.3.4. Vulnerabilidades

"Se refiere a una debilidad en un sistema informático permitiendo a un atacante violar el control de acceso y a la confidencialidad de datos y aplicaciones. Las vulnerabilidades son el resultado de fallos en el diseño o desarrollo o a las propias limitaciones del sistema" (SeguridadPC.Net, 2016)

2.3.5. Amenazas

Se puede definir como amenaza a todo elemento o acción capaz de atentar contra la seguridad de la información.

"Las amenazas surgen a partir de la existencia de vulnerabilidades, es decir que una amenaza sólo puede existir si existe una vulnerabilidad que pueda ser aprovechada, e independientemente que se comprometa o no la seguridad de un sistema de información" (Departamento de Seguridad Informática, 2016)

Las amenazas se dividen en dos grupos:

Internas: Estas son las más peligrosas, ya que siempre se origina por alguien que se encuentra dentro de la organización, resultando difícil de mitigar por las siguientes razones:

Tienen conocimiento de la red y saben cómo funcionan. Tienen un nivel de acceso a la red por las mismas necesidades de su trabajo. Queda imposibilitado el IPS (Sistema de Prevención de Intrusos) y Firewall, debido a que viene de dentro de la misma organización.

Externas: Estas amenazas son realizadas por personas externas que laboran fuera de la organización, pues logran ingresar a través de la red, principalmente desde internet, buscando dañar, alterar, o eliminar información de la organización.

2.3.6. Riesgo

Es la probabilidad de que una amenaza se origine, dando lugar a un ataque a la organización.

Según de Organización Internacional por la Normalización (ISO) define riesgo tecnológico como: "La probabilidad que una amenaza se materialice, utilizando una o más vulnerabilidades existentes de un activo o grupo de activos, generando pérdidas o daños"

El riesgo involucra:

Incertidumbre: Es una situación en la cual no se tiene la certeza de que ocurrirá determinado evento.

Pérdida Potencial: "Son las fallas o deficiencias en los sistemas, en los controles internos o por errores en el procesamiento de las operaciones" (Afore, 2016)

2.3.7. Salvaguarda

Se definen las salvaguardas o contra medidas como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo.

2.4. Antecedentes del Problema

2.4.1. Antecedentes Internacionales

(Yangua, 2014) En su tesis **"**Auditoría Informática y su Incidencia en los Riesgos para el Manejo de la Información en la Cooperativa de Ahorro y Crédito Educadores de Tungurahua**"** concluye que:

La entidad donde ella realizó su trabajo de investigación tiene poca conciencia acerca de la importancia de la seguridad de la información y de los riesgos que están expuestos al no aplicar políticas de seguridad, esto se debe gran parte al desinterés de los funcionarios que tienen una mentalidad de que ellos no están expuestos a riesgos que generen problemas en lo que respecta a la seguridad de la información.

Además, recomienda el uso de la metodología MAGERIT para disminuir los riesgos para el manejo de la información, la cual consiste en el análisis y gestión de riesgos, ayudando a saber el valor de la información y protegerla.

(Perafán & Caicedo, 2014) En su tesis "Análisis de Riesgos de la Seguridad de la Información para la Institución Universitaria Colegio Mayor Del Cauca" concluyen que:

Aplicar un análisis de riesgos permite conocer de manera global el estado actual de la seguridad informática dentro de la Institución, además de dejar una propuesta de políticas de seguridad para ser tomadas como soporte de la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI).

Estos autores recomiendan usar la metodología MAGERIT para el análisis de riesgos, ya que este nos ayuda a dar el primer paso para garantizar la seguridad informática dentro de la institución.

2.4.2. Antecedentes Nacionales

(García, 2016) en su tesis "Implementación de un Sistema de Gestión de Seguridad de la Información, aplicado a los riesgos asociados a los activos de información en la empresa NET – Consultores S.A.C" concluye que:

La implementación de un Sistema de Gestión de Seguridad de la Información permite minimizar los riesgos asociados a los activos de información, pero que la empresa debe estar preparada para actuar de manera inmediata ante cualquier eventualidad que pueda poner en peligro el normal funcionamiento y el futuro de la empresa, debido a que constantemente se presentan más activos de información, más riesgos o amenazas.

(Guevara, 2015) en su tesis "Aplicación de la Metodología MAGERIT para el Análisis y Gestión de Riesgos en los Servidores de los Sistemas de Gestión Académica de la Universidad Nacional Pedro Ruiz Gallo", concluye que:

Los servidores de los sistemas de gestión académica tienen medidas de seguridad implantadas, pero no se encuentran ni guiadas ni documentadas por lo que no son adecuadamente aprovechadas.

Utilizó la metodología MAGERIT y la herramienta Pilar las cuales fueron de ayuda para el análisis y gestión de riesgos, concluyendo que los servidores estaban expuestos a un riesgo crítico mediante amenazas como: caída del sistema por agotamiento de recursos, avería de origen físico o lógico, corte de suministro eléctrico, robo de equipos, pérdida de equipos, errores humanos.

Además, este autor elaboró de un plan de mitigación, que se realizó tomando en cuenta factores de seguridad, la importancia de los

activos y los servidores de gestión académica como principal objetivo de su investigación.

2.5. Marco Legal

2.5.1. Norma ISO/IEC 27000

Familia de estándares donde especifica claramente los parámetros sobre seguridad de la información, para desarrollar, implementar y mantener los sistemas de gestión de seguridad de la información, entre ellos:

Norma ISO/IEC 27001: Define los requisitos para la implementación de un SGSI (Sistema de Gestión de la Seguridad de la Información).

Norma ISO/IEC 27002: (anterior ISO 17799). Es una guía de buenas prácticas, describe los controles a seguir dentro del marco de la seguridad de la información; enmarcados en 11 dominios, 39 objetivos de control y 133 controles.

Norma ISO/IEC 27003: Proporciona ayuda y orientación sobre la implementación de un SGSI, incluye el método PHVA (planear, hacer verificar y actuar) contribuyendo con revisiones y mejora continua.

Norma ISO/IEC 27004: Especificará las métricas y técnicas de medición para determinar la eficacia de un SGSI y de sus controles. Aplicable específicamente en la fase del hacer (Do); de acuerdo con el método PHVA.

Norma ISO/IEC 27005: Suministra directrices para la gestión del riesgo en la seguridad de la información.

2.5.2. Norma Técnica Peruana

NTP-ISO/IEC 27001:2014 (INDECOPI, 2014), esta Norma Técnica Peruana especifica los requisitos para establecer implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información dentro del contexto de la organización. Esta Norma Técnica Peruana también incluye requisitos para la evaluación y tratamiento de los riesgos de seguridad de la información orientados a las necesidades de la organización. Los requisitos establecidos en esta Norma Técnica Peruana son genéricos y están hechos para aplicarse a todas las organizaciones, sin importar su tipo, tamaño o naturaleza.

2.5.3. Ley de Delitos Informáticos

Ley N°30096 (Congreso del Perú, 2013) Esta Ley peruana tiene como objetivo prevenir y sancionar las conductas ilícitas que afectan a los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidos mediante la utilización de tecnologías de la información o de la comunicación, con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia.

2.5.4. Ley de Protección de Datos Personales

Ley N° 29733 (PCM, 2016) de Protección de Datos Personales del Perú tiene como objetivo proteger todos los datos de las personas naturales gestionados por las compañías: clientes, colaboradores y proveedores, entre otros. Para ello se requiere la implementación de un marco integrado de medidas técnicas, organizacionales y legales.

CAPÍTULO III

METODOLOGÍA MAGERIT

CAPITULO III – METODOLOGÍA MAGERIT.

3.1. Introducción

En la actualidad la Administración Pública y Privada depende de forma creciente de los Sistemas de Información para alcanzar sus objetivos. El uso de las tecnologías de información y telecomunicaciones (TIC) supone un beneficio evidente para los usuarios, pero esto también da lugar a ciertos riesgos que se deben gestionar prudentemente con medidas de seguridad que sustente la confianza de los usuarios de estos servicios.

MAGERIT es el acrónimo de "Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información" creado por el Consejo Superior de Administración Electrónica (CSAE). El uso de esta metodología es de carácter público, pertenece al Ministerio de Administraciones Públicas (MAP) de España.

La Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, es un método formal para conocer los riesgos a los cuales están expuestos los Activos de Información, y para recomendar las medidas apropiadas que deberían adoptarse para mitigar estos riesgos.

3.2. Historia y Evolución

Actualmente esta metodología se encuentra en su tercera versión, la primera versión fue publicada en 1997, la cual ha subsistido en su mayor parte el paso del tiempo. Sin embargo, este intervalo de tiempo ha permitido mejorar notablemente esta primera versión.

La segunda versión fue publicada en 2005, la cual fue una revisión constructiva, adaptándose al su tiempo e incorporando experiencias de los ochos años anteriores desde la primera versión.

Actualmente, la tercera versión busca una nueva adaptación, teniendo en cuenta no solo la experiencia práctica, sino también la evolución de las normas internacionales de ISO que constituyen un referente muy importante.

3.3. Objetivos de MAGERIT

MAGERIT persigue los siguientes objetivos.

Directos:

1.- Concientizar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.

2.- Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC)

3.- Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control

Indirectos:

4.- Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda cada caso.

3.4. Metodología MAGERIT 3.0

Siguiendo la terminología de la normativa ISO 31000, MAGERIT responde a lo que se denomina "Proceso de Gestión de los Riesgos", sección 4.4 ("Implementación de la Gestión de los Riesgos") dentro del "Marco de Gestión de Riesgos". En otras palabras, MAGERIT implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información.

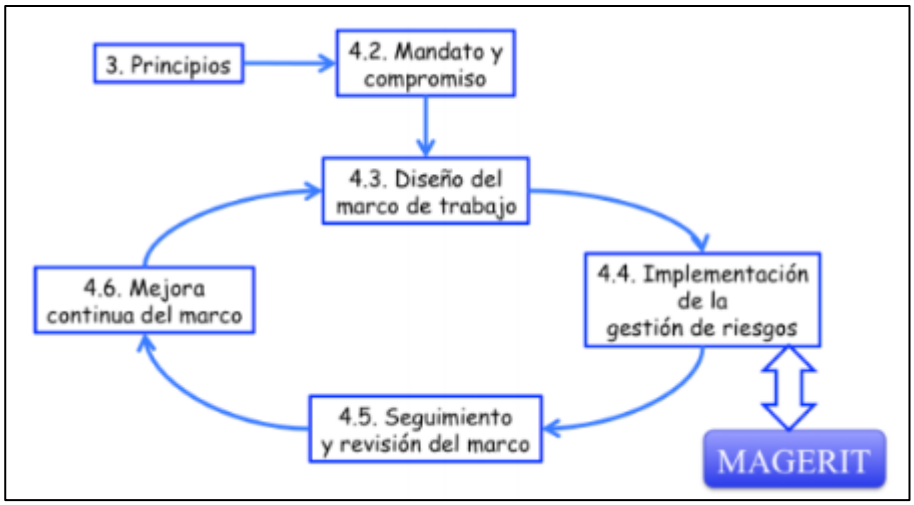


Gráfico 02: ISO 31000 – Marco de trabajo para la gestión de riesgos
Fuente: Libro 1 de MAGERIT 3.0

Existen varias aproximaciones que sirven para analizar los riesgos que pueden sufrir los sistemas y las tecnologías de la información y telecomunicaciones: guías formales, aproximaciones metódicas y herramientas de soporte. Todas ellas tienen como finalidad el saber cuan seguros o inseguros son los sistemas. Existen muchos elementos que hay que considerar para lograr tener buenos resultados. Es por ello que MAGERIT está basado sobre una aproximación metódica que no deja lugar a la improvisación, ni dependa de la arbitrariedad del analista.

Los resultados que se dan después de realizar el análisis de riesgos aplicando esta metodología permite la gestión de los riegos recomendando las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y reducir el impacto que se generaría al ser materializados.

3.4.1. Organización de las Guías.

La Metodología consta de tres volúmenes:

Volumen I: Método
Volumen II: Catálogo de Elementos.

Volumen III: Guía de Técnicas.

3.4.2. Volumen I: Método

Esta guía está estructura de la siguiente manera:

Capítulo I: Es una fase introductoria a esta metodología, pronunciando que organismos lo crearon.

Capítulo II: **Visión de Conjunto**, presenta los conceptos informalmente. Particularmente se enmarcan las actividades de análisis y tratamiento de riesgos para tener un proceso integral de gestión de riesgos.

Capítulo III: **Método de Análisis de Riesgos**, es exclusivo solo para el Análisis de Riesgos donde explica detalladamente cada uno de los pasos que se van a realizar en este tipo de proyectos, donde va orientado para cualquier organización empresarial que lo requiera.

Capítulo IV: **Proceso de Gestión de Riesgos**, describe todas las actividades que se hacen dentro de la Gestión de Riesgos.

Capítulo V: **Proyectos de Análisis de Riesgos**, se centra en los Proyectos de Análisis de Riesgos, proyectos en los que nos veremos inmersos para realizar el primer análisis de riesgos de un sistema y eventualmente cuando hay cambios sustanciales y hay que rehacer el modelo ampliamente.

Capítulo VI: **Plan de Seguridad**, determina cuáles serán las actividades para llevar a cabo un Plan de Seguridad, después de haber realizado el proyecto de Análisis y Gestión de Riesgos, de esta manera se escogen las decisiones apropiadas para el tratamiento de los riesgos.

Capítulo VII: **Desarrollo de Sistemas de Información**, se centra la seguridad de los sistemas de información considerando varios puntos de vista para mitigar riesgos, además interviene el Análisis de Riesgos que tiene el mismo propósito asegurar la información.

Capítulo VIII: **Consejos Prácticos**, ofrece recomendaciones prácticas para aplicarlos en las tareas del Análisis de Riesgos, lo que resulta muy conveniente para la persona que realiza este tipo de proyectos.

3.4.3. Volumen II: Catálogo de Elementos

Complementa el volumen I proporcionando tareas que sirve para aplicación de esta metodología. Proporciona información en cuando a:

- Tipos de activos
- Dimensiones y criterios de valoración
- Amenazas
- Salvaguardas

En este libro se establecen dos objetivos:

1. Facilitar la labor de las personas que ejecutan el proyecto, en el sentido de ofrecerles elementos estándar a los que puedan adscribirse rápidamente, centrándose en lo específico del sistema objeto del análisis.

2. Homogeneizar los resultados de los análisis, promoviendo una terminología y unos criterios uniformes que permitan

comparar e incluso integrar análisis realizados por diferentes equipos.

3.4.4. Volumen III: Guía de técnicas.

El objetivo de este documento es describir algunas técnicas utilizadas en análisis y gestión de riesgos. Se considera técnica a un conjunto de heurísticos y procedimientos que ayudan a alcanzar los objetivos propuestos.

Para cada una de las técnicas referenciadas:

- Se explica brevemente el objetivo que se persigue al utilizarlas,
- Se describen los elementos básicos asociados,
- Se exponen los principios fundamentales de elaboración,
- Se presenta una notación textual y/o gráfica y
- Y se citan las fuentes bibliográficas que, sin ser exhaustivas, se han estimado de interés para que el lector profundice en cada materia.

Las técnicas que recoge son:

- Análisis mediante tablas
- Análisis algorítmico
- Árboles de ataque
- Técnicas generales
- Análisis coste-beneficio
- Diagramas de flujo de datos (DFD)
- Diagramas de procesos
- Técnicas gráficas
- Sesiones de trabajo: Entrevistas, reuniones y presentaciones.
- Valoración Delphi.

3.5. Método de Análisis de Riesgo.

El análisis de riesgos es una aproximación metódica para determinar el riesgo siguiendo unos pasos pautados:

- Determinar los activos relevantes para la Organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación.

- Determinar a qué amenazas están expuestos aquellos activos.

- Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo.

- Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.

- Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza.

3.6. Proceso de Gestión de Riesgos.

El análisis de riesgos determina impactos y riesgos, este resultado es solo un análisis. A partir de esto disponemos de información para tomar decisiones conociendo lo que queremos proteger (Activos) y que se ha hecho hasta ese momento para protegerlo (Salvaguarda).

En este paso, las decisiones son de los encargados por la administración de estos activos. En el gráfico siguiente se resume las posibles decisiones que se pueden tomar tras haber estudiado los riesgos.

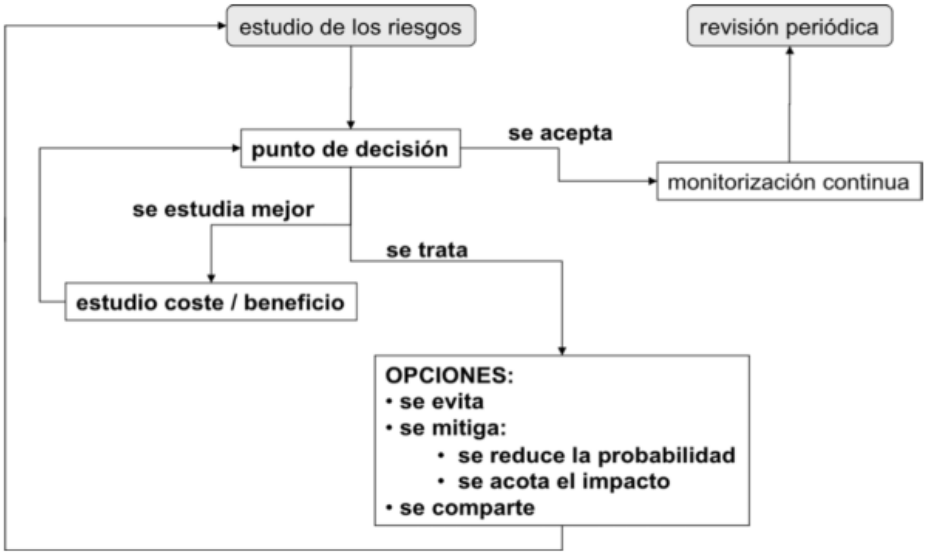


Gráfico 03: Decisiones para el tratamiento de los riesgos
Fuente: Libro 1 de MAGERIT 3.0

3.7. Plan de Mejora

En esta fase se trata de llevar a cabo los planes de seguridad, de acuerdo a las decisiones acogidas por el tratamiento de los riesgos. Para llevar a cabo este proceso de identifican 3 tareas fundamentales.

1.- Identificación de proyectos de seguridad.
2.- Plan de ejecución.
3.- Ejecución.

En última instancia se trata de implantar o mejorar una serie de salvaguardas que lleven el impacto y los riesgos a los niveles determinados por los Administradores de la Institución.

3.8. Justificación de la metodología MAGERIT

Para la realización de un Análisis de Gestión de Riesgos existen varias guías informales, aproximaciones metódicas, estándares y herramientas se soporte que buscan gestionar y mitigar los riesgos. Anteriormente en la sección del marco teórico de este proyecto, ya se hizo mención de algunas de las

metodologías existentes en el mercado actual. Para justificar el uso de la metodología MAGERIT se realizó el siguiente cuadro comparativo.

		MAGERIT	OCTAVE	CRAMM	EBIOS
Alcance Considerado	Análisis de Riesgos	Si	Si	Si	Si
	Gestión de Riesgos	Si	Si	Si	Si
Tipo de Análisis	Cuantitativo	Si	Limitada	Si	Si
	Cualitativo	Si	Limitada	Si	Si
	Mixto	Si	Limitada	Si	No
Objetivos de Seguridad	Confidencialidad	Si	Si	Si	Si
	Integridad	Si	Si	Si	Si
	Disponibilidad	Si	Si	Si	Si
	Autenticidad	Si	No	No	No
	Trazabilidad	Si	No	No	No
Ayudas a la Implantación	Herramienta	Si	No	Limitada	Si
	Plan de Proyecto	Si	Si	Limitada	No
	Técnicas	Si	Si	No	No
	Roles	Si	Si	Si	No
	Comparativas	Si	No	Si	No

Tabla 02: Comparativa de Metodologías
Fuente: Elaboración Propia basado en estudios comparativos de la metodología, usando como principal fuente la tesis de Marquina, año 2010. Pag 19.

3.9. Herramienta PILAR

PILAR, es el acrónimo de "Procedimiento Informático-Lógico para el Análisis de Riesgos" es una herramienta desarrollada por el Centro Nacional de Inteligencia para soportar el Análisis de Riesgos de Sistemas de Información basado en la metodología MAGERIT.

En esta herramienta se puede hacer todas las actividades que se realizan en el Análisis y Gestión de Riesgos:

- Determinación de Activos: Identificación, dependencias y valoración.
- Determinación de Amenazas
- Estimación de Impactos
- Determinación de los criterios de aceptación del riesgo
- Determinación de las medidas de seguridad necesarias o Salvaguardas.

Este software permite hacer un Análisis de Riesgos sobre las dimensiones de valoración como son: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad. Además, nos ayuda con el cálculo del impacto y el riesgo, acumulado, repercutido, potencial y residual.

"Las salvaguardas se califican por fases, permitiendo la incorporación a un mismo modelo de diferentes situaciones temporales. Típicamente se puede incorporar el resultado de los diferentes proyectos de seguridad a lo largo de la ejecución del plan de seguridad, monitorizando la mejora del sistema." (Dirección General de Modernización Administrativa, 2017)

CAPÍTULO IV

DESARROLLO DEL ANÁLISIS DE RIESGOS.

CAPITULO IV – DESARROLLO DEL ANÁLISIS DE RIESGO.

4.1. Equipo de trabajo.

Este trabajo se realizó por tres personas. El tesista, Cristhian Briceño Huaygua, quien estuvo asesorado por el Ing. Rigo Felix Requena Flores, además del Jefe del área de informática, Ing. Guillermo Oswaldo Morán Girón, quien fue muy importante para la recopilación de información de los activos y la valoración de estos, además de que, a través de entrevistas y observación directa, ayudó a conocer las amenazas que están expuestos estos activos, los riesgos, y las salvaguardas con las que cuenta actualmente la Institución.

4.2. Alcance.

El presente proyecto consistió en identificar los principales riesgos a los que están expuestos actualmente los activos de información de la ZED PAITA, siguiendo la metodología MAGERIT.

Los análisis fueron de orden cualitativo, usando los niveles de medición en orden a la escala dado por la metodología, se determinaron los activos y amenazas en forma general considerando los prioritarios para el buen funcionamiento de la Institución, los salvaguardas se definieron sin considerar el costo económico, ya que para el estudio no se dio acceso a los datos financieros, por lo tanto el resultado de este proyecto, solo sirve de guía para la institución y las personas encargadas, las cuales lo evaluarán antes de implementarlo o mejorarlo.

Se usó la herramienta PILAR en modo de evaluación, ya que la licencia tiene un costo que fue asumido por ninguna de las partes involucradas, el único

inconveniente sobre este, fue que no se generaron los reportes automáticamente, lo cual se corrigió realizándolos manualmente.

Al desarrollar este proyecto, su finalidad fue demostrar que la Institución y la mayoría de instituciones de la Administración pública aún no toman conciencia de los riesgos a los que están expuestos los activos de información, además de no contar con un Plan de contingencia, de tal manera que puedan minimizar el impacto que genera la materialización de una amenaza. De tal manera se propone un Plan de Mejora de la seguridad de los activos de Información.

4.3. Situación Actual.

La Zona Especial de Desarrollo – ZED PAITA, cuenta con un área cercada de 20 hectáreas, dentro de esta área se encuentran más de quince empresas que alquilan un lote para desarrollas diferentes tipos de actividades.

El cerco perimetral tiene dos puertas de acceso, una para entrada de vehículos y otra para salida de estos mismos, además de una puerta de acceso peatonal reguardada por una garita de control. Todo personal que ingresa es debidamente identificado, dejando su DNI y recibiendo un pase de acceso.

Para el presente proyecto sólo se tomó en cuenta el edificio administrativo el cual cuenta con una sola planta, en el interior se divide con tres áreas, el área de Secretaría General, el área de Administración y el Área de informática. Además de un área de Balanza, que se encuentra fuera del edificio administrativo, al costado de la puerta de ingreso de vehículos.

4.3.1. Equipos informáticos.

En el área de informática se encuentran los servidores principales, actualmente se cuenta con un Firewall de la marca Sophos, un servidor de base de Datos, un servidor de Aplicaciones, un Swicth, un Router y una central telefónica analógica. Estos equipos están en un gabinete el cual está a vista de cualquiera que ingresa a esta área.

El área de administración cuenta con computadores de escritorio, de las cuales dos de ellas usan el Sistema Operativo Windows 8, cuatro computadoras usan Windows 7, y dos usan Windows XP.

En el área de balanza hay una computadora con Windows 7, la cual es usada por dos operadores, cada uno con su usuario y contraseña, en diferentes horarios.

4.3.2. Aplicaciones.

La Institución trabaja con un Sistema de Información principal llamado Sistema de Gestión, el cual contiene entre sus módulos, el módulo de importadores, el módulo de Transportistas, el módulo de Salidas de Mercancías, el módulo de Productos, el módulo de Clientes, y el módulo de Planillas.

Casi el 90 % de los procesos de la institución están soportados por este sistema, el cual ha sido programa en Visual Basic 6.0, según las entrevistas que se realizaron, este sistema contiene errores a la hora de generar los reportes que se requieren.

También hay un Sistema de Visitas, el cual sólo es utilizado en la garita de Control para registrar las mercancías que están ingresando a la Institución, estos ingresos no se reflejan en el Sistema de Gestión, por lo cual se evidencia un doble esfuerzo en esta tarea repetitiva.

Las computadoras están gestionadas con End Points, por un antivirus Sophos, el cual se debe actualizar manualmente por el encargado del área de informática.

4.3.3. Equipamiento Auxiliar.

La institución cuenta con un UPS el cual tiene una latencia de 2 horas, además cuenta con un Grupo Electrógeno el cual recibe mantenimiento cada vez que presenta alguna falla, no se cuenta con un cronograma de fecha establecido para los mantenimientos, si se tiene conciencia de los mantenimientos correctivos.

Todos los ambientes cuentan con Aire Acondicionado, incluso en el área de informática se mantiene la temperatura más baja, por el motivo de la presencia del gabinete, con el inconveniente que los que se encuentran en esa área están a la misma temperatura que recibe el gabinete, ya que este no cuenta con un cuarto especial.

4.3.4. Redes de comunicación.

La institución cuenta con una conexión a internet contratada a un tercero, internamente las computadoras se conectan a través de una red cableado y una red WiFi, los accesos a la red inalámbrica son controlados por el encargado del área de informática, además existen una conexión VPN la cual sólo es usada por el encargado del área para conexiones externas.

4.3.5. Personal.

Los principales actores que participan en los procesos de la empresa son los siguientes:

El Encargado del área de informática, el cual vela que todos los procesos informáticos se desarrollen con normalidad.

Dos operadores en el área de balanza, los cuales son los responsables del ingreso de la información al Sistema de Gestión, la cual será usada por todas las demás áreas.

Los usuarios finales, aquí se abarca todos los usuarios de los Sistemas de información, para el desarrollo del presente proyecto, se agrupa en un solo bloque.

4.4. Caso de Estudio – Análisis de Riesgos

Para realizar una Plan de Mejora de los activos de información seguiremos las siguientes actividades, de acuerdo con la Metodología MAGERIT.

1.- Identificar y valorar los activos de información de la Institución

2.- Identificar y valorar las amenazas a las que están expuestos estos activos de información.

3.- Identificar las salvaguardas actuales con las que cuenta la Institución.

4.- Evaluar el impacto posible sobre los procesos de la Institución si es que alguna amenaza se materializa.

5.- Informar a los encargados y proponer un Plan de Mejora para una buena gestión de los riesgos y tomar decisiones con motivos justificados.

El análisis se realizó usando la Herramienta Pilar, la cual ya se describió anteriormente, de esta manera se tuvo una guía en el proyecto realizado. Pilar nos sirve de ayuda en la identificación y valorización de activos, amenazas y salvaguardas. Con los resultados obtenidos, se redactó el Plan de Mejora que se propone a la Institución.

4.4.1. Datos del Proyecto.

Código: PDM – ZED PAITA

Nombre: Diseño de un Plan de Mejora de la seguridad de información – ZED PAITA

Descripción: Aplicación de la Metodología Magerit para la elaboración de un Plan de Mejora.

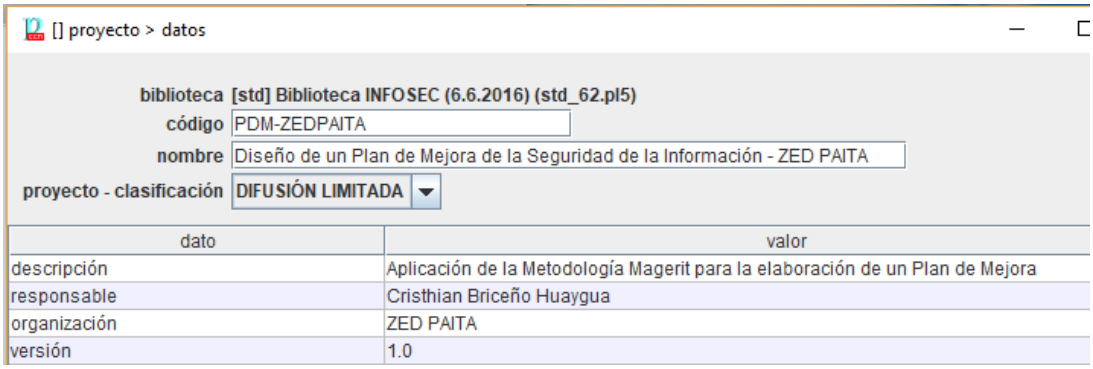


Gráfico 04: Datos de Proyecto.
Fuente: Herramienta Pilar 6.2.6

4.4.2. Identificación de Activos.

Es el primer paso que dicta la metodología, esta tarea se culminó satisfactoriamente, dando como resultado la siguiente tabla.

TIPO	NOMBRE DEL ACTIVO
SERVICIOS	1. [SERV_TEL] Servicio de Telefonía analógica
	2. [SERV_CORREO] Servicio de Correo Institucional
	3. [SERV_SOPORTE] Servicio de soporte técnico
APLICACIONES	4. [SI_GESTION] Sistema de Gestión
	5. [SI_VISITAS] Sistema de Visitas
	6. [SO] Sistema Operativo
	7. [ANT_VIR] Antivirus
EQUIPAMIENTO INFORMATICO	8. [SRV_FIRE] Servidor de Firewall
	9. [SRV_BD] Servidor Base de datos
	10. [SRV_APP] Servidor de Aplicaciones
	11. [SWICHT] Switch
	12. [CENTRAL_TEL] Central telefónica
	13. [IMP] Impresoras
	14. [ROUT] Router
	15. [PC] Computadoras de escritorio
REDES DE COMUNICACIONES	16. [ADSL] Conexión a internet
	17. [WIFI] Conexión Inalámbrica
	18. [LAN] Conexión LAN
	19. [VPN] Conexión VPN
EQUIPAMIENTO AUXILIAR	20. [CAB_RED] Cableado de Red
	21. [UPS] UPS
	22. [GRP_ELEC] Grupo electrógeno
INSTALACIONES	23. [LOCAL_INF] Área de Informática
	24. [LOCAL_ADM] Área de Administración
	25. [LOCAL_BAL] Área de Balanza
PERSONAL	26. [JEFE_TI] jefe de TI
	27. [OPER] Operadores de Balanza
	28. [USERS] Usuarios Finales

Tabla 03: Identificación de activos
Fuente: Elaboración Propia

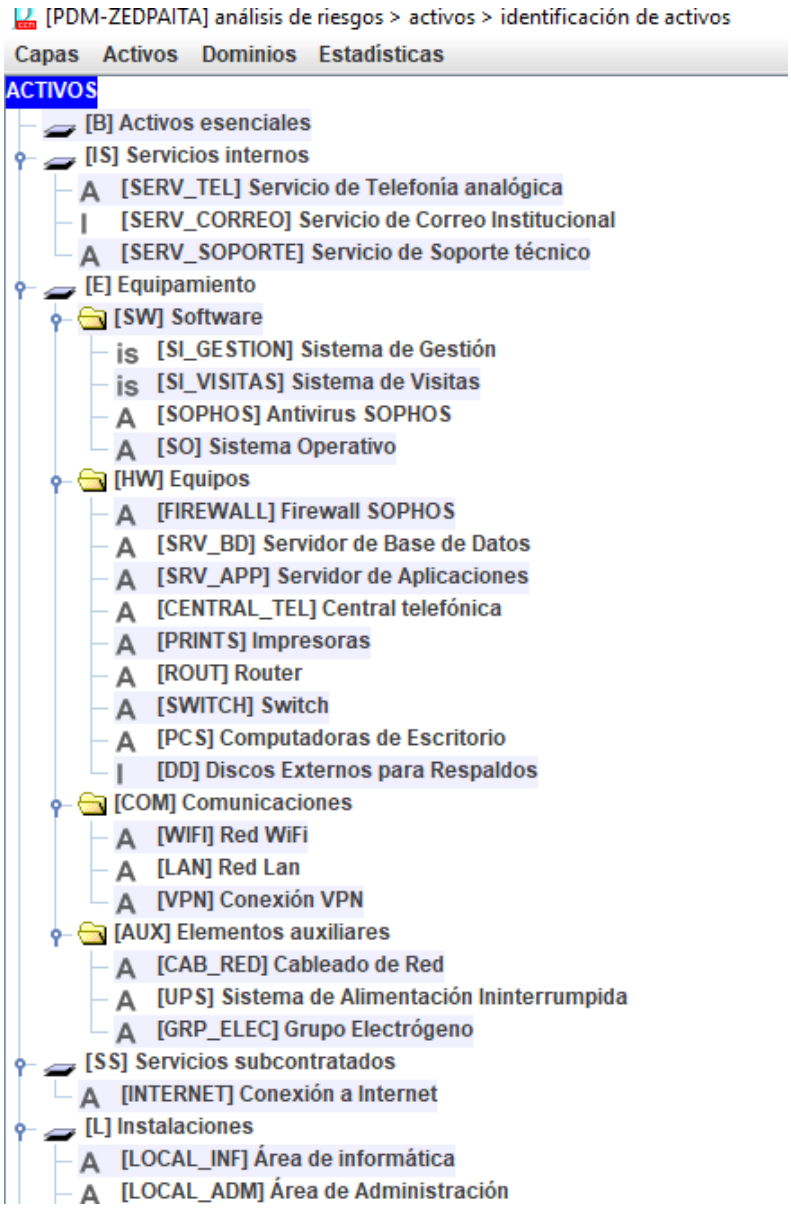


Gráfico 05: Identificación de activos
Fuente: Herramienta Pilar 6.2.6

4.4.3. Valoración de los Activos.

Esta tarea tiene como objetivo principal identificar en que dimensiones el activo es valioso para el correcto funcionamiento de los procesos de la Institución. Es muy importante tener en cuenta que un activo interesa por lo que vale.

Para cada valoración se tiene en cuenta las dimensiones y los criterios.

Criterios de valoración.

Valor		Criterio
10	Extremo	Daño extremadamente grave
9	Muy Alto	Daño muy grave
6 - 8	Alto	Daño grave
3 - 5	Medio	Daño importante
1 - 2	Bajo	Daño menor
0	Despreciable	Irrelevante a efectos prácticos

Tabla 04: Criterios de valoración
Fuente: Libro 02 – Catálogo de Elementos - MAGERIT

Dimensiones

- **[D]** Disponibilidad
- **[I]** Integridad de los datos
- **[C]** Confidencialidad de los datos
- **[A]** Autenticidad de los usuarios y de la información

Para el presente proyecto, se dieron valor a los activos, a través de observación directa, con apoyo del Encargado de área de Informática. Dando como resultado la siguiente tabla:

ACTIVOS	[D]	[I]	[C]	[A]
Servicios Internos				
[SERV_TEL] Servicio de Telefonía analógica	[5]	[5]	[5]	[8]
[SERV_CORREO] Servicio de Correo Institucional	[8]	[7]	[6]	[9]
[SERV_SOPORTE] Servicio de soporte técnico	[3]			
Aplicaciones				
[SI_GESTION] Sistema de Gestión	[10][1]	[9]	[9]	[9]
[SI_VISITAS] Sistema de Visitas	[10] [1]	[9]	[8]	[8]
[SO] Sistema Operativo	[8]	[4]	[4]	[5]
[ANT_VIR] Antivirus	[8]	[7]	[4]	[5]
Equipos				
[SRV_FIRE] Firewall SOPHOS	[8]	[7]	[4]	[8]

[SRV_BD] Servidor Base de datos	[10] [1]	[10]	[9]	[9]
[SRV_APP] Servidor de Aplicaciones	[10] [1]	[9]	[9]	[9]
[SWICHT] Switch	[9]		[2]	[7]
[CENTRAL_TEL] Central telefónica	[5]	[5]		[5]
[IMP] Impresoras	[5]			
[ROUT] Router	[8]		[2]	[7]
[PC] Computadoras de escritorio	[6]		[2]	[7]
[DD] Disco externos para respaldos	[4]	[9]	[9]	[9]
Redes de Comunicación				
[INTERNET] Conexión a internet	[7]	[6]	[2]	[4]
[WIFI] Conexión Inalámbrica	[5]	[5]	[5]	[3]
[LAN] Conexión LAN	[9]	[5]	[5]	[5]
[VPN] Conexión VPN	[3]	[9]	[5]	[9]
Equipos Auxiliares				
[CAB_RED] Cableado de Red	[8] [1]	[8]		
[UPS] UPS	[4]	[7]		
[GRP_ELEC] Grupo electrógeno	[4]	[9]		
Instalaciones				
[LOCAL_INF] Área de Informática	[8]	[9]	[2]	[9]
[LOCAL_ADM] Área de Administración	[9]	[7]	[2]	[5]
[LOCAL_BAL] Área de Balanza	[10] [2]	[10]	[4]	[8]
Personal				
[JEFE_TI] Jefe de TI	[9]	[8]	[5]	[8]
[OPER] Operadores de Balanza	[8] [2]	[8]	[5]	[8]
[USERS] Usuarios Finales	[7]	[4]	[2]	[5]

Tabla 05: Valor propio de los activos
Fuente: Elaborado por el autor y el jefe del área de informática

(1) Podría causar la interrupción de actividades propias de la Institución

(2) Pudiera impedir las operaciones de la Institución

4.4.4. Identificación de las amenazas.

El objetivo de esta tarea es identificar las amenazas a las que están expuestos los activos de la Institución. MAGERIT clasifica las amenazas en cuatro grupos.

- [N] Desastres Naturales
- [I] De Origen Industrial
- [E] Errores y fallos no intencionados

- [A] Ataques intencionados

En la tabla siguiente se identifican las amenazas relevantes sobre casa activo de la Institución.

Activos	**Amenazas**
Telefonía analógica	[I.5] Avería de origen físico o lógico [I.6] Corte del suministro eléctrico [E.1] Errores de los usuarios [E.2] Errores del administrador del sistema. [E.19] Fugas de información. [E.23] Errores de mantenimiento [A.5] Suplantación de la identidad [A.7] Uso no previsto. [A.14] Intercepción de información (escucha). [A.23] Manipulación de hardware [A.24] Denegación de servicio [A.25] Robo de equipos [A.26] Ataque destructivo
Servicio de Correo Institucional	[I.5] Avería de origen físico o lógico [I.6] Corte del suministro eléctrico [E.1] Errores de los usuarios [E.2] Errores del administrador del sistema. [E.8] Difusión de software dañino [E.15] Alteración de la Información [E.18] Destrucción de la información. [E.19] Fugas de información. [E.20] Vulnerabilidades de los programas. [E.23] Errores de mantenimiento [E.24] Caída del sistema por agotamiento de recursos. [A.5] Suplantación de la identidad [A.7] Uso no previsto. [A.8] Difusión de software dañino. [A.11] Acceso no autorizado [A.15] Modificación de la información [A.18] Destrucción de la información. [A.24] Denegación de servicio
Servicio de soporte técnico	[E.18] Destrucción de la información. [E.28] Indisponibilidad del personal [A.18] Destrucción de la información. [A.28] Indisponibilidad del personal [A.29] Extorsión

	[A.30] Ingeniería social (picaresca)
Sistema de Gestión	[I.5] Avería de origen físico o lógico [I.6] Corte del suministro eléctrico [E.1] Errores de los usuarios [E.2] Errores del administrador del sistema. [E.15] Alteración de la Información [E.18] Destrucción de la información. [E.19] Fugas de información. [E.20] Vulnerabilidades de los programas. [E.21] Errores de mantenimiento [E.28] Indisponibilidad del personal. [E.24] Caída del sistema por agotamiento de recursos. [A.5] Suplantación de la identidad [A.6] Abuso de privilegio de acceso. [A.7] Uso no previsto. [A.8] Difusión de software dañino. [A.11] Acceso no autorizado [A.15] Modificación de la información [A.18] Destrucción de la información. [A.19] Revelación de información. [A.24] Denegación de servicio [A.28] Indisponibilidad del personal.
Sistema de Visitas	[I.5] Avería de origen físico o lógico [I.6] Corte del suministro eléctrico [E.1] Errores de los usuarios [E.2] Errores del administrador del sistema. [E.15] Alteración de la Información [E.18] Destrucción de la información. [E.19] Fugas de información. [E.20] Vulnerabilidades de los programas. [E.21] Errores de mantenimiento [E.28] Indisponibilidad del personal. [E.24] Caída del sistema por agotamiento de recursos. [A.5] Suplantación de la identidad [A.7] Uso no previsto. [A.11] Acceso no autorizado [A.15] Modificación de la información [A.18] Destrucción de la información. [A.19] Revelación de información. [A.24] Denegación de servicio [A.28] Indisponibilidad del personal.
Sistema Operativo	[I.5] Avería de origen físico o lógico

	[E.8 Difusión de Software dañino [E.20] Vulnerabilidades de los programas. [E.21] Errores de mantenimiento [A.8] Difusión de software dañino. [A.22] Manipulación de programas.
Antivirus	[I.5] Avería de origen físico o lógico [E.8 Difusión de Software dañino [E.18] Destrucción de la información. [E.19] Fugas de información. [E.20] Vulnerabilidades de los programas. [E.21] Errores de mantenimiento [A.15] Modificación de la información [A.18] Destrucción de la información. [A.22] Manipulación de programas.
Firewall SOPHOS	[N.*] Desastres naturales [I.1] Fuego [I.2] Daño por agua. [I.5] Avería de origen físico o lógico [I.6] Corte del suministro eléctrico [I.7] Condiciones inadecuadas de temperatura. [E.2] Errores del administrador del sistema. [E.23] Errores de mantenimiento [E.24] Caída del sistema por agotamiento de recursos. [A.11] Acceso no autorizado [A.23] Manipulación de hardware [A.25] Robo de equipos. [A.26] Ataque destructivo
Servidor Base de datos	[N.*] Desastres naturales [I.1] Fuego [I.2] Daño por agua. [I.5] Avería de origen físico o lógico [I.6] Corte del suministro eléctrico [I.7] Condiciones inadecuadas de temperatura. [E.2] Errores del administrador del sistema. [E.4] Errores de configuración [E.18] Destrucción de la información [E.19] Fugas de información [E.23] Errores de mantenimiento [E.24] Caída del sistema por agotamiento de recursos. [A.3] Manipulación de los registros de

	actividad [A.4] Manipulación de los ficheros de configuración [A.5] Suplantación de identidad [A.6] Abuso de privilegios de acceso [A.7] Uso no previsto [A.11] Acceso no autorizado [A.24] Denegación de servicio. [A.25] Robo de equipos. [A.26] Ataque destructivo
Servidor de Aplicaciones	[N.*] Desastres naturales [I.1] Fuego [I.2] Daño por agua. [I.5] Avería de origen físico o lógico [I.6] Corte del suministro eléctrico [I.7] Condiciones inadecuadas de temperatura. [E.2] Errores del administrador del sistema. [E.3] Errores de monitorización (log) [E.4] Errores de configuración [E.8] Difusión de software dañino [E.18] Destrucción de la información [E.19] Fugas de información [E.20] Vulnerabilidades de los programas. [E.23] Errores de mantenimiento [E.24] Caída del sistema por agotamiento de recursos. [A.3] Manipulación de los registros de actividad [A.4] Manipulación de los ficheros de configuración [A.5] Suplantación de identidad [A.6] Abuso de privilegios de acceso [A.7] Uso no previsto [A.8] Difusión de software dañino [A.15] Modificación de la información [A.18] Destrucción de la información [A.22] Manipulación de programas [A.23] Manipulación de hardware [A.24] Denegación de servicio. [A.25] Robo de equipos. [A.26] Ataque destructivo
Switch	[N.*] Desastres naturales [I.1] Fuego [I.2] Daño por agua.

	[I.5] Avería de origen físico o lógico [I.6] Corte del suministro eléctrico [I.7] Condiciones inadecuadas de temperatura. [E.2] Errores del administrador del sistema. [E.4] Errores de configuración [A.23] Manipulación de hardware [A.25] Robo de equipos. [A.26] Ataque destructivo
Central telefónica	[N.*] Desastres naturales [I.1] Fuego [I.2] Daño por agua. [I.5] Avería de origen físico o lógico [I.6] Corte del suministro eléctrico [I.7] Condiciones inadecuadas de temperatura. [E.23] Errores del mantenimiento [A.11] Acceso no autorizado [A.23] Manipulación de hardware [A.25] Robo de equipos. [A.26] Ataque destructivo
Impresoras	[N.*] Desastres naturales [I.1] Fuego [I.2] Daño por agua. [I.5] Avería de origen físico o lógico [I.6] Corte del suministro eléctrico [E.23] Errores del mantenimiento [E.4] Errores de configuración [A.23] Manipulación de hardware [A.25] Robo de equipos. [A.26] Ataque destructivo
Router	[N.*] Desastres naturales [I.1] Fuego [I.2] Daño por agua. [I.5] Avería de origen físico o lógico [I.6] Corte del suministro eléctrico [I.7] Condiciones inadecuadas de temperatura. [E.2] Errores del administrador del sistema. [E.4] Errores de configuración [A.11] Acceso no autorizado [A.23] Manipulación de hardware [A.25] Robo de equipos. [A.26] Ataque destructivo

Computadoras de escritorio	[N.*] Desastres naturales [I.1] Fuego [I.2] Daño por agua. [I.5] Avería de origen físico o lógico [I.6] Corte del suministro eléctrico [I.7] Condiciones inadecuadas de temperatura. [E.23] Errores del mantenimiento [A.7] Uso no previsto [A.11] Acceso no autorizado [A.23] Manipulación de hardware [A.25] Robo de equipos. [A.26] Ataque destructivo
Disco externos para respaldos	[N.*] Desastres naturales [I.1] Fuego [I.2] Daño por agua. [I.5] Avería de origen físico o lógico [I.7] Condiciones inadecuadas de temperatura. [E.15] Alteración de la información [E.18] Destrucción de la información [E.19] Fugas de información [E.25] Pérdidas de equipos [A.11] Acceso no autorizado [A.25] Robo de equipos. [A.26] Ataque destructivo
Conexión a internet	[I.8] Fallo en el servicio de comunicaciones [E.9] Errores de re-encaminamiento [E.19] Fugas de información [E.24] Caída del sistema por agotamiento de recursos. [A.5] Suplantación de la identidad [A.7] Uso no previsto [A.11] Acceso no autorizado [A.12] Análisis de tráfico [A.14] Interceptación de mensajes (escucha) [A.15] Modificación de la información [A.18] Destrucción de la información [A.24] Denegación de servicio
Conexión Inalámbrica	[I.8] Fallo en el servicio de comunicaciones [E.2] Errores del administrador del sistema [E.24] Caída del sistema por agotamiento de recursos. [A.7] Uso no previsto

	[A.9] Re-encaminamiento de mensajes. [A.11] Acceso no autorizado [A.12] Análisis de tráfico [A.14] Interceptación de mensajes (escucha) [A.15] Modificación de la información [A.18] Destrucción de la información [A.24] Denegación de servicio
Conexión LAN	[I.8] Fallo en el servicio de comunicaciones [E.2] Errores del administrador del sistema [E.19] Fugas de información [A.5] Suplantación de la identidad [A.7] Uso no previsto [A.9] Re-encaminamiento de mensajes. [A.11] Acceso no autorizado [A.12] Análisis de tráfico [A.14] Interceptación de mensajes (escucha) [A.15] Modificación de la información [A.18] Destrucción de la información [A.24] Denegación de servicio
Conexión VPN	[I.8] Fallo en el servicio de comunicaciones [E.2] Errores del administrador del sistema [E.15] Alteración de la información [E.19] Fugas de información [E.24] Caída del sistema por agotamiento de recursos. [A.5] Suplantación de la identidad [A.7] Uso no previsto [A.11] Acceso no autorizado [A.12] Análisis de tráfico [A.18] Destrucción de la información [A.24] Denegación de servicio
Cableado de Red	[N.2] Daño por agua [N.*] Desastres naturales [I.1] Fuego [E.23] Errores de mantenimiento [A.23] Manipulación del hardware [A.26] Ataque destructivo
UPS	[N.2] Daño por agua [N.*] Desastres naturales [I.1] Fuego [E.23] Errores de mantenimiento

	[A.7] Uso no previsto [A.23] Manipulación del hardware [A.25] Robo de equipos [A.26] Ataque destructivo
Grupo electrógeno	[N.2] Daño por agua [N.*] Desastres naturales [I.1] Fuego [I.9] Interrupción de suministros [E.23] Errores de mantenimiento [A.7] Uso no previsto [A.23] Manipulación del hardware [A.25] Robo de equipos [A.26] Ataque destructivo
Área de Informática Área de Administración Área de Balanza	[N.2] Daño por agua [N.*] Desastres naturales [I.1] Fuego [I.3] Contaminación medioambiental [A.6] Abuso de privilegio de acceso [A.7] Uso no previsto [A.26] Ataque destructivo [A.27] Ocupación enemiga
Jefe de TI Operadores de Balanza Usuarios Finales	[E.15] Alteración de la información [E.18] Destrucción de la información [E.19] Fugas de información [E.28] Indisponibilidad del personal [A.15] Modificación de la información [A.18] Destrucción de la información [A.19] Revelación de información [A.28] Indisponibilidad del personal [A.29] Extorsión [A30] Ingeniería social (picaresca)

Tabla 06: Identificación de amenazas
Fuente: Elaborado por el autor y el jefe del área de informática, basado en las amenazas comunes que propone la herramienta PILAR 6.2.6

4.4.5. Valorización de las amenazas.

En esta tarea se determina la influencia en el valor del activo si es que una amenaza llegaría a materializarse. Se evalúa la probabilidad de ocurrencia y se estima la degradación que causaría la amenaza en cada dimensión del activo.

La probabilidad de ocurrencia es compleja de determinar, ya que es difícil saber en qué momento se puede materializar una amenaza, para el siguiente proyecto se modelará cualitativamente por medio de la siguiente escala

CS	Casi seguro
MA	Muy alto
P	Posible
PP	Poco probable
MR	Muy raro

Tabla 07: Probabilidad de ocurrencia
Fuente: Libro 1 – Metodología Magerit

La degradación significa el daño causado por el incidente, para el siguiente proyecto se usará los valores propuestos por MAGERIT.

En la tabla siguiente se muestra la frecuencia de acuerdo a la escala escogida, y la degradación en cada una de las dimensiones de los activos de la Institución.

Activos	**Amenazas**	**FR.**	**D**	**I**	**C**	**A**
Telefonía analógica	[I.5] Avería de origen físico o lógico	P	50%			
	[I.6] Corte del suministro eléctrico	P	100%			
	[E.1] Errores de los usuarios	P	10%	10%	10%	
	[E.2] Errores del administrador del sistema.	P	20%	20%	20%	
	[E.19] Fugas de información.	P			10%	
	[E.23] Errores de mantenimiento	P	10%			
	[A.5] Suplantación de la identidad	P		50%	50%	100%
	[A.7] Uso no previsto.	P	1%	10%	10%	

	[A.14] Intercepción de información (escucha).	MR				
	[A.23] Manipulación de hardware	P	50%		50%	
	[A.24] Denegación de servicio	PP	100%			
	[A.25] Robo de equipos	PP	100%		50%	
	[A.26] Ataque destructivo	MR	100%			
Servicio de Correo Institucional	[I.5] Avería de origen físico o lógico	P	50%			
	[I.6] Corte del suministro eléctrico	P				
	[E.1] Errores de los usuarios	P	10%	10%	10%	
	[E.2] Errores del administrador del sistema.	P	20%	20%	20%	
	[E.8] Difusión de software dañino	P	10%	10%	10%	
	[E.15] Alteración de la Información	P		1%		
	[E.18] Destrucción de la información.	P	10%			
	[E.19] Fugas de información.	P			10%	
	[E.20] Vulnerabilidades de los programas.	P	1%	20%	20%	
	[E.23] Errores de mantenimiento /Actualización del Software	MA	1%	1%		
	[E.24] Caída del sistema por agotamiento de recursos.	P	50%			
	[A.5] Suplantación de la identidad	P		50%	50%	100%
	[A.6] Abuso de privilegios de acceso	P	1%	10%	10%	100%
	[A.7] Uso no previsto.	P	1%	10%	10%	
	[A.8] Difusión de software dañino.	P	1%	100%	100%	
	[A.11] Acceso no autorizado	P		10%	50%	100%
	[A.15] Modificación de la información	P		50%		
	[A.18] Destrucción de la información.	P	50%			
	[A.24] Denegación de servicio	P	50%			
Servicio de soporte técnico	[E.18] Destrucción de la información.	P	1%			

	[E.28] Indisponibilidad del personal	P	10%			
	[A.18] Destrucción de la información.	P	10%			
	[A.28] Indisponibilidad del personal	P	20%			
	[A.29] Extorsión	P	50%			
	[A.30] Ingeniería social (picaresca)	P	50%			
Sistema de Gestión	[I.5] Avería de origen físico o lógico	P	50%			
	[I.6] Corte del suministro eléctrico	P	100%			
	[E.1] Errores de los usuarios	P	10%	10%	10%	
	[E.2] Errores del administrador del sistema.	P	20%	20%	20%	
	[E.15] Alteración de la Información	P		10%		
	[E.18] Destrucción de la información.	P	1%			
	[E.19] Fugas de información.	P			10%	
	[E.20] Vulnerabilidades de los programas.	P	1%	20%	20%	
	[E.21] Errores de mantenimiento	MA	1%	1%		
	[E.28] Indisponibilidad del personal.	P	50%			
	[E.24] Caída del sistema por agotamiento de recursos.	P	30%			
	[A.5] Suplantación de la identidad	MA		50%	50%	100%
	[A.6] Abuso de privilegio de acceso.	P	1%	10%	10%	100%
	[A.7] Uso no previsto.	P	1%	10%	10%	
	[A.11] Acceso no autorizado	P		10%	50%	100%
	[A.15] Modificación de la información	MA		50%		
	[A.18] Destrucción de la información.	P	10%			
	[A.19] Revelación de información.	MA			50%	
	[A.24] Denegación de servicio	P	50%			
	[A.28] Indisponibilidad del personal.	P	50%			

Sistema de Visitas	[I.5] Avería de origen físico o lógico	P	50%			
	[I.6] Corte del suministro eléctrico	P	100%			
	[E.1] Errores de los usuarios	P	10%			
	[E.2] Errores del administrador del sistema.	P	1%			
	[E.15] Alteración de la Información	P		10%		
	[E.18] Destrucción de la información.	P	1%			
	[E.19] Fugas de información.	P			10%	
	[E.20] Vulnerabilidades de los programas.	P	1%	20%	20%	
	[E.21] Errores de mantenimiento	MA	1%	1%		
	[E.28] Indisponibilidad del personal.	P	30%			
	[E.24] Caída del sistema por agotamiento de recursos.	P	50%			
	[A.5] Suplantación de la identidad	-				
	[A.7] Uso no previsto.	-				
	[A.11] Acceso no autorizado	-				
	[A.15] Modificación de la información	P		50%		
	[A.18] Destrucción de la información.	P	10%			
	[A.19] Revelación de información.	MA			50%	
	[A.24] Denegación de servicio	P				
	[A.28] Indisponibilidad del personal.	P	50%			
Sistema Operativo	[I.5] Avería de origen físico o lógico	P	50%			
	[E.8 Difusión de Software dañino	P	10%	10%	10%	
	[E.20] Vulnerabilidades de los programas.	MA	1%	20%	20%	
	[E.21] Errores de mantenimiento	MA	1%	1%		
	[A.8] Difusión de software dañino.	P	100%	100%	100%	
	[A.22] Manipulación de programas.	P	50%	100%	100%	

Antivirus	[I.5] Avería de origen físico o lógico	P	50%			
	[E.8 Difusión de Software dañino	P	10%	10%	10%	
	[E.18] Destrucción de la información.	P	1%			
	[E.19] Fugas de información.	P			10%	
	[E.20] Vulnerabilidades de los programas.	P	1%	20%	20%	
	[E.21] Errores de mantenimiento	MA	1%	1%		
	[A.15] Modificación de la información	P		50%		
	[A.18] Destrucción de la información.	P	10%			
	[A.22] Manipulación de programas.	P	50%	100%	100%	
Firewall SOPHOS	[N.*] Desastres naturales	PP	100%			
	[I.1] Fuego	P	100%			
	[I.2] Daño por agua.	P	50%			
	[I.5] Avería de origen físico o lógico	P	50%			
	[I.6] Corte del suministro eléctrico	P	100%			
	[I.7] Condiciones inadecuadas de temperatura.	P	100%			
	[E.2] Errores del administrador del sistema.	-				
	[E.23] Errores de mantenimiento	P	10%			
	[E.24] Caída del sistema por agotamiento de recursos.	P	50%			
	[A.11] Acceso no autorizado	P	10%	10%	50%	
	[A.23] Manipulación de hardware	P	50%		50%	
	[A.25] Robo de equipos.	PP	100%		100%	
	[A.26] Ataque destructivo	P	100%			
Servidor Base de datos	[N.*] Desastres naturales	PP	100%			
	[I.1] Fuego	P	100%			
	[I.2] Daño por agua.	MR	100%			

	[I.5] Avería de origen físico o lógico	P	50%			
	[I.6] Corte del suministro eléctrico	P	100%			
	[I.7] Condiciones inadecuadas de temperatura.	P	100%			
	[E.2] Errores del administrador del sistema.	PP	10%			
	[E.4] Errores de configuración	P		1%		
	[E.18] Destrucción de la información	P	1%			
	[E.19] Fugas de información	P			50%	
	[E.23] Errores de mantenimiento	P	10%			
	[E.24] Caída del sistema por agotamiento de recursos.	MA	50%			
	[A.3] Manipulación de los registros de actividad	P		50%		
	[A.4] Manipulación de los ficheros de configuración	P	10%	10%	10%	
	[A.5] Suplantación de identidad	MA		10%	50%	100%
	[A.6] Abuso de privilegios de acceso	P	10%	100%	100%	
	[A.7] Uso no previsto	P	10%	10%	100%	
	[A.11] Acceso no autorizado	P	10%	100%	100%	
	[A.24] Denegación de servicio.	P	100%			
	[A.25] Robo de equipos.	P	100%		100%	
	[A.26] Ataque destructivo	P	100%			
Servidor de Aplicaciones	[N.*] Desastres naturales	PP	100%			
	[I.1] Fuego	PP	100%			
	[I.2] Daño por agua.	PP	50%			
	[I.5] Avería de origen físico o lógico	P	50%			
	[I.6] Corte del suministro eléctrico	P	100%			
	[I.7] Condiciones inadecuadas de temperatura.	P	100%			
	[E.2] Errores del administrador del sistema.	P	20%	20%	20%	
	[E.3] Errores de monitorización	P		1%		

	(log)					
	[E.4] Errores de configuración	P		1%		
	[E.8] Difusión de software dañino	P	10%	10%	10%	
	[E.18] Destrucción de la información	P	10%			
	[E.19] Fugas de información	P			10%	
	[E.20] Vulnerabilidades de los programas.	P	1%	20%	20%	
	[E.23] Errores de mantenimiento	MA	10%	1%		
	[E.24] Caída del sistema por agotamiento de recursos.	P	50%			
	[A.3] Manipulación de los registros de actividad	P		50%		
	[A.4] Manipulación de los ficheros de configuración	MA	10%	10%	10%	
	[A.5] Suplantación de identidad	P		50%	50%	100%
	[A.6] Abuso de privilegios de acceso	P	1%	10%	10%	100%
	[A.7] Uso no previsto	P	1%	1%	10%	
	[A.8] Difusión de software dañino	P	100%	100%	100%	
	[A.15] Modificación de la información	P		50%		
	[A.18] Destrucción de la información	P	50%			
	[A.22] Manipulación de programas	P	50%	100%	100%	
	[A.23] Manipulación de hardware	P	50%		50%	
	[A.24] Denegación de servicio.	P	100%			
	[A.25] Robo de equipos.	PP	100%		100%	
	[A.26] Ataque destructivo	P	100%			
Switch	[N.*] Desastres naturales	PP	100%			
	[I.1] Fuego	P	100%			
	[I.2] Daño por agua.	P	50%			
	[I.5] Avería de origen físico o lógico	P	50%			
	[I.6] Corte del suministro eléctrico	P	100%			

	[I.7] Condiciones inadecuadas de temperatura.	P	100%			
	[E.2] Errores del administrador del sistema.	-				
	[E.4] Errores de configuración	-				
	[A.23] Manipulación de hardware	P	100%		50%	
	[A.25] Robo de equipos.	P	20%		50%	
	[A.26] Ataque destructivo	P	100%			
Central telefónica	[N.*] Desastres naturales	PP	100%			
	[I.1] Fuego	PP	100%			
	[I.2] Daño por agua.	P	50%			
	[I.5] Avería de origen físico o lógico	P	50%			
	[I.6] Corte del suministro eléctrico	P	100%			
	[I.7] Condiciones inadecuadas de temperatura.	P	100%			
	[E.23] Errores del mantenimiento	P	10%			
	[A.11] Acceso no autorizado	P	10%	10%		
	[A.23] Manipulación de hardware	P	50%			
	[A.25] Robo de equipos.	P	100%			
	[A.26] Ataque destructivo	P	100%			
Impresoras	[N.*] Desastres naturales	PP	100%			
	[I.1] Fuego	PP	100%			
	[I.2] Daño por agua.	MA	50%			
	[I.5] Avería de origen físico o lógico	P	50%			
	[I.6] Corte del suministro eléctrico	P	100%			
	[E.23] Errores del mantenimiento	P	10%			
	[A.23] Manipulación de hardware	P	50%			
	[A.25] Robo de equipos.	P	100%			
	[A.26] Ataque destructivo	P	100%			
Router	[N.*] Desastres naturales	PP	100%			

	[I.1] Fuego	MR	100%			
	[I.2] Daño por agua.	P	50%			
	[I.5] Avería de origen físico o lógico	P	50%			
	[I.6] Corte del suministro eléctrico	P	100%			
	[I.7] Condiciones inadecuadas de temperatura.	P	100%			
	[E.2] Errores del administrador del sistema.	P		50%		
	[E.4] Errores de configuración	P		50%		
	[A.11] Acceso no autorizado	P	10%		50%	
	[A.23] Manipulación de hardware	P	100%		50%	
	[A.25] Robo de equipos.	P	20%		50%	
	[A.26] Ataque destructivo	P	100%			
Computadoras de escritorio	[N.*] Desastres naturales	PP	100%			
	[I.1] Fuego	P	100%			
	[I.2] Daño por agua.	P	50%			
	[I.5] Avería de origen físico o lógico	P	50%			
	[I.6] Corte del suministro eléctrico	P	100%			
	[I.7] Condiciones inadecuadas de temperatura.	P	100%			
	[E.23] Errores del mantenimiento	P	10%			
	[A.7] Uso no previsto	P	10%		10%	
	[A.11] Acceso no autorizado	P	10%		50%	
	[A.23] Manipulación de hardware	P	50%		50%	
	[A.25] Robo de equipos.	P	5%		10%	
	[A.26] Ataque destructivo	P	100%			
Disco externos para respaldos	[N.*] Desastres naturales	PP	100%			
	[I.1] Fuego	PP	50%			
	[I.2] Daño por agua.	P	50%			
	[I.5] Avería de origen físico o lógico	P	50%			

	[I.7] Condiciones inadecuadas de temperatura.	P	100%			
	[E.15] Alteración de la información	P		1%		
	[E.18] Destrucción de la información	P	1%			
	[E.19] Fugas de información	P			10%	
	[E.25] Pérdidas de equipos	P	100%		50%	
	[A.11] Acceso no autorizado	P	10%	10%	50%	
	[A.25] Robo de equipos.	P	100%		50%	
	[A.26] Ataque destructivo	P	100%			
Conexión a internet	[I.8] Fallo en el servicio de comunicaciones	P	50%			
	[E.9] Errores de re-encaminamiento	P			10%	
	[E.19] Fugas de información	P			10%	
	[E.24] Caída del sistema por agotamiento de recursos.	P	50%			
	[A.5] Suplantación de la identidad	P		10%	50%	100%
	[A.7] Uso no previsto	P	10%	10%	10%	
	[A.11] Acceso no autorizado	P		10%	50%	100%
	[A.12] Análisis de tráfico	P			2%	
	[A.14] Interceptación de mensajes (escucha)	P			5%	
	[A.15] Modificación de la información	P		10%		
	[A.18] Destrucción de la información	P	50%			
	[A.24] Denegación de servicio	MA	50%			
Conexión Inalámbrica	[I.8] Fallo en el servicio de comunicaciones	P	50%			
	[E.2] Errores del administrador del sistema	P	20%	20%	20%	
	[E.24] Caída del sistema por agotamiento de recursos.	P	50%			
	[A.7] Uso no previsto	P	10%	10%	10%	
	[A.9] Re-encaminamiento de mensajes.	P			10%	
	[A.11] Acceso no autorizado	P		10%	50%	100%
	[A.12] Análisis de tráfico	P			2%	

	[A.14] Interceptación de mensajes (escucha)	P			10%	
	[A.15] Modificación de la información	P		10%		
	[A.18] Destrucción de la información	P	50%			
	[A.24] Denegación de servicio	MA	50%			
Conexión LAN	[I.8] Fallo en el servicio de comunicaciones	P	50%			
	[E.2] Errores del administrador del sistema	P	20%	20%	20%	
	[E.19] Fugas de información	P			10%	
	[A.5] Suplantación de la identidad	P		10%	50%	100%
	[A.7] Uso no previsto	P	10%	10%	10%	
	[A.9] Re-encaminamiento de mensajes.	P			10%	
	[A.11] Acceso no autorizado	P		10%	50%	100%
	[A.12] Análisis de tráfico	P			2%	
	[A.14] Interceptación de mensajes (escucha)	P			1%	
	[A.15] Modificación de la información	P		10%		
	[A.18] Destrucción de la información	P	50%			
	[A.24] Denegación de servicio	MA	50%			
Conexión VPN	[I.8] Fallo en el servicio de comunicaciones	P	50%			
	[E.2] Errores del administrador del sistema	P	20%	20%	20%	
	[E.15] Alteración de la información	P		1%		
	[E.19] Fugas de información	P			10%	
	[E.24] Caída del sistema por agotamiento de recursos.	P	50%			
	[A.5] Suplantación de la identidad	P		10%	50%	100%
	[A.7] Uso no previsto	P	10%	10%	10%	
	[A.11] Acceso no autorizado	P		10%	50%	100%
	[A.12] Análisis de tráfico	PP			2%	
	[A.18] Destrucción de la información	PP	50%			

	[A.24] Denegación de servicio	MA	50%			
Cableado de Red	[N.2] Daño por agua	PP	50%			
	[N.*] Desastres naturales	PP	100%			
	[I.1] Fuego	P	100%			
	[E.23] Errores de mantenimiento	P	10%			
	[A.23] Manipulación del hardware	P	50%			
	[A.26] Ataque destructivo	P	100%			
UPS	[N.2] Daño por agua	PP	1%			
	[N.*] Desastres naturales	PP	1%			
	[I.1] Fuego	P	1%			
	[E.23] Errores de mantenimiento	P	1%			
	[A.7] Uso no previsto	P	1%	0%		
	[A.23] Manipulación del hardware	P	1%			
	[A.25] Robo de equipos	PP	1%			
	[A.26] Ataque destructivo	P	1%			
Grupo electrógeno	[N.2] Daño por agua	PP	1%			
	[N.*] Desastres naturales	PP	1%			
	[I.1] Fuego	P	1%			
	[I.9] Interrupción de suministros	P	1%			
	[E.23] Errores de mantenimiento	P	1%			
	[A.7] Uso no previsto	P	1%	0%		
	[A.23] Manipulación del hardware	P	1%			
	[A.25] Robo de equipos	PP	1%			
	[A.26] Ataque destructivo	P	1%			
Área de Informática Área de Administración Área de Balanza	[N.2] Daño por agua	P	100%			
	[N.*] Desastres naturales	PP	100%			
	[I.1] Fuego	P	100%			
	[I.3] Contaminación medioambiental	P	10%			

	[A.6] Abuso de privilegio de acceso	P	10%			
	[A.7] Uso no previsto	P	10%			
	[A.26] Ataque destructivo	PP	100%			
	[A.27] Ocupación enemiga	PP	100%			
Jefe de TI Operadores de Balanza Usuarios Finales	[E.15] Alteración de la información	P		10%		
	[E.18] Destrucción de la información	P	1%			
	[E.19] Fugas de información	P			10%	
	[E.28] Indisponibilidad del personal	P	10%			
	[A.15] Modificación de la información	P		50%		
	[A.18] Destrucción de la información	P	10%			
	[A.19] Revelación de información	MA			50%	
	[A.28] Indisponibilidad del personal	P	20%			
	[A.29] Extorsión	PP	50%	100%	100%	
	[A30] Ingeniería social (picaresca)	PP	50%	100%	100%	

Tabla 08: Valorización de las amenazas
Fuente: Realizado por el autor y el jefe del área de informática, con la ayuda de la herramienta Pilar 6.2.6

4.4.6. Caracterización de las salvaguardas.

En esta tarea se identifican las salvaguardas efectivas para la Institución junto con la eficacia que tienen cada una de ellas para mitigar los riesgos. Las salvaguardas son medidas, procedimientos o mecanismos que reducen el riesgo de que una amenaza se materialice.

	aspecto	tdp	salvaguarda	dudas	fuente	comentario	recomendación	on / off
			SALVAGUARDAS					
	G	EL	[IA] Identificación y autenticación				8	
	T	EL	[AC] Control de acceso lógico				7	
	G	PR	[D] Protección de la Información				8	
	G	EL	[K] Protección de claves criptográficas					
	G	PR	[S] Protección de los Servicios				6	
	G	PR	[SW] Protección de las Aplicaciones Informáticas (SW)				7	
	G	PR	[HW] Protección de los Equipos Informáticos (HW)				7	
	G	PR	[COM] Protección de las Comunicaciones				9	
	G	PR	[IP] Sistema de protección de frontera lógica					
	G	PR	[MP] Protección de los Soportes de Información					
	G	PR	[AUX] Elementos Auxiliares				6	
	F	PR	[L] Protección de las Instalaciones				7	
	F	EL	[PPS] Protección del perímetro físico					
	P	PR	[PS] Gestión del Personal				6	
	G	PR	[PDS] Servicios potencialmente peligrosos					
	G	CR	[IR] Gestión de incidentes				6	
	T	PR	[tools] Herramientas de seguridad				9	
	G	CR	[V] Gestión de vulnerabilidades				6	
	T	MN	[A] Registro y auditoría				7	
	G	RC	[BC] Continuidad del negocio				5	
	G	AD	[G] Organización				5	
	G	AD	[E] Relaciones Externas				6	
	G	AD	[NEW] Adquisición / desarrollo				5	

Gráfico 06: Identificación de salvaguardas
Fuente: Libro II - Catálogo de elementos, Metodología Magerit, visualización en la Herramienta Pilar 6.2.6

Aspecto que trata la salvaguarda:

Abreviatura	**Aspecto**
G	Para Gestión
T	Para Técnico
F	Para Seguridad Física
P	Para Gestión del Personal

Tabla 09: Aspecto de las Salvaguardas
Fuente: Herramienta Pilar 6.2.6

Tipo de protección.:

Abreviatura	**Tipo de protección**
PR	Prevención
EL	Eliminación
CR	Corrección
MN	Monitorización
RC	Recuperación

Tabla 10: Tipo de Protección

Fuente: Herramienta Pilar 6.2.6

AD	Administrativa

Pesos relativos:

	máximo peso	crítica
	peso alto	muy importante
	peso normal	importante
	peso bajo	interesante
	aseguramiento: componentes certificados	

Gráfico 07: Peso relativo de las salvaguardas
Fuente: Herramienta Pilar 6.2.6

4.4.7. Identificación de las salvaguardas existentes.

El objetivo de esta tarea es identificar las salvaguardas actuales con las que cuenta la institución para protegerse de la materialización de alguna amenaza y de esta manera trata de mitigar el riesgo al que está expuesto.

Se usará la nomenclatura propuesta por la herramienta Pilar 6.2.6 de acuerdo a una escala definida, explicada en la siguiente tabla.

Nivel	**Madurez**
L0	Inexistente

L1	Inicial
L2	Reproducible, pero intuitivo
L3	Proceso definido
L4	Gestionado y medible
L5	Optimizado

Tabla 11: Niveles de madurez
Fuente: Herramienta Pilar 6.2.6

Amenaza	**Salvaguarda**	**Actual**	**Objetivo**
Fuego	Instalación de sistema contra incendios	L2	L4
	Instalación de alarmas contra incendio	L0	L4
	Uso y mantenimiento de extintores	L3	L4
	Desarrollo de plan de emergencia ante incendios	L1	L3
Desastres naturales	Desarrollo de plan de emergencia ante desastres	L0	L3
	Realización de simulacros de forma periódica	L0	L3
	Almacenamiento de Discos de respaldo en otra oficina	L3	L3
Agotamiento de recursos	Mantenimiento preventivo de servidores	L2	L4
	Revisión de directiva de copias de seguridad de forma regular	L0	L3
	Monitoreo de recursos de los equipos críticos	L2	L4
Errores de configuración	Realizar pruebas de actualización previa la instalación	L1	L3
	Pruebas periódicas del Firewall	L0	L3
Desconexión física o lógica	Asegurar los equipos de comunicaciones y servidores en armarios cerrados	L1	L3
Vulnerabilidades de Software	Se actualizan los programas regularmente (Sistemas operativos.)	L1	L3
Robo	Uso de cables de seguridad para computadoras	L0	L3
	Uso de cámaras de seguridad en lugares	L2	L4

	estratégicos		
Virus	Instalación de antivirus en servidores	L3	L4
	Instalación de antivirus en equipos personales	L4	L4
	Actualización periódica de firmas de antivirus	L4	L4
Malware	Instalación de antimalware en servidores	L0	L3
	Instalación de antimalware en equipos personales	L0	L3
Fallas de generador eléctrico	Mantenimiento mensual del generador eléctrico	L2	L4
Acceso no autorizado	Establecer controles de acceso físico	L3	L3
	Analizar directivas de cortafuegos	L1	L3
	Implementación de sistema de detección de intrusos	L0	L3
	Asignar cuentas para la administración de sistemas	L3	L3
	Utilizar autenticación multifactor para conexión remota	L0	L3
	Implementar control de cuarentena en VPN	L0	L3
	Implementar directiva de contraseñas complejas	L0	L3
Fuga de información	Implementación de cifrado de datos	L0	L3
	Contratación de personal responsable de seguridad informática	L0	L3
	Solicitar historial de personal antes de ser contratado	L2	L3
	Dar charlas al personal referente a la seguridad	L1	L3

Tabla 12: Evaluación de Salvaguardas
Fuente: Elaborado por el autor y el jefe del área de informática, basado en la metodología Magerit.

En la tabla anterior se tienen las salvaguardas que indican el nivel de madurez actual de la Institución. En el nivel L0 se han

considerado los procedimientos inexistentes y que aún no han sido evaluados.

- Desarrollo de un plan de contingencia ante desastres naturales
- Realizar simulacros de forma periódica.
- Desarrollar procesos de planificación de capacidad de TI, desarrollo seguro, pruebas de seguridad siguiendo los estándares de seguridad internacionales.
- Coordinar una revisión periódica de las copias de seguridad y de las reglas de acceso configuradas en el Firewall para verificar que estas funcionen en óptimas condiciones.
- Iniciar el uso de cables de seguridad para los equipos de cómputo.
- La implementación de un sistema de detección de intrusos.
- Agregar la seguridad al acceso remoto utilizando autenticación de dos factores.
- Contratación de personal responsable de la seguridad, quien se encargará de documentar los procedimientos, normas y directrices de seguridad de la información, identificar los roles y responsabilidades que deben asignarse al personal administrativo, esto debe tener participación conjunta con la gerencia.

En los niveles L1 y L2 se consideran los procedimientos existentes pero que aún falta mejorar su gestión, como son los referentes de seguridad física, dentro del plan de emergencia ante incendios es necesario definir a los responsables y los procedimientos necesarios para llevar a cabo la restauración de la información respaldada. A continuación, se proponen mejoras a las salvaguardas actuales para una mejor gestión.

- Adquirir la buena práctica de realizar pruebas de las actualizaciones previas a su instalación en los servidores, hacer un seguimiento continuo a los parches de seguridad mediante herramientas de escaneo de vulnerabilidades para su posterior actualización.

- Analizar las directivas del Firewall con regularidad asegurando el nivel de protección equilibrado de la red perimetral.

- Asignar cuentas dedicadas a la administración con contraseñas complejas y que sean cambiadas de forma regular para reducir el riesgo de accesos no autorizados.

- Actualizar los sistemas operativos, debido a que los sistemas operativos antiguos dejan de tener soporte y son vulnerables a ataques deliberados.

- Para evitar la fuga de información sería recomendable investigar un poco más sobre el nuevo personal a contratar, solicitando referencias a los centros de trabajo anteriores, además de clasificar la información para dar a conocer los datos a los que deben de conocer y que no llegue a personal no autorizado.

Las salvaguardas con nivel L3 y L4 son aquellas que están siendo implementadas de forma correcta y que podrían optimizarse para mejorar la seguridad física y lógica. Los niveles objetivos son L4 y L5, pero siempre teniendo en cuenta que se debe optimizar los procedimientos de protección.

4.4.8. Valoración de las salvaguardas

Con ayuda de la herramienta Pilar, se ingresa los niveles que se realizó en la fase anterior para que la herramienta pueda procesar los datos y mostrarnos el riesgo e impacto que generar las amenazas y de qué manera son mitigadas por las salvaguardas actuales, además nos servirá para que más adelante se pueda mostrar los riesgos e impactos acumulados y residuales.

[PDM-ZEDPAITA] análisis de riesgos > salvaguardas > Eficacia de las salvaguardas

Editar Expandir Exportar Importar Estadísticas

[base] Base

aspecto	tdp	salvaguarda	come...	reco...		Actual	Objetivo	PILAR
		SALVAGUARDAS						
G	EL	[IA] Identificación y autenticación		8		L3	L4	L2-L5
T	EL	[AC] Control de acceso lógico		7		L2	L4	L2-L4
G	PR	[D] Protección de la Información		8		L2	L4	L2-L5
G	PR	[S] Protección de los Servicios		6		L2	L4	L2-L4
G	PR	[SW] Protección de las Aplicaciones Informáticas (SW)		7		L3	L3	L2-L4
G	PR	[HW] Protección de los Equipos Informáticos (HW)		7		L2	L4	L2-L4
G	PR	[COM] Protección de las Comunicaciones		9		L2	L4	L2-L5
G	PR	[MP] Protección de los Soportes de Información						
G	PR	[AUX] Elementos Auxiliares		6		L2	L4	L2-L4
F	PR	[L] Protección de las Instalaciones		7		L2	L4	L2-L4
F	EL	[PPS] Protección del perímetro físico						
P	PR	[PS] Gestión del Personal		6		L2	L4	L2-L4
G	CR	[IR] Gestión de incidentes		6		L0	L3	L2-L4
T	PR	[tools] Herramientas de seguridad		9		L2	L4	L2-L5
G	CR	[V] Gestión de vulnerabilidades		6		L1	L4	L2-L4
T	MN	[A] Registro y auditoría		7		L1	L3	L2-L4
G	RC	[BC] Continuidad del negocio		5		L2	L3	L2-L3
G	AD	[G] Organización		5		L1	L3	L2-L3

Gráfico 08: Evaluación de las salvaguardas
Fuente: Herramienta Pilar 6.2.6

La columna "Recomendación" indica la valoración de la salvaguarda teniendo en cuento el tipo de activo, el rango es de 0 a 10, en las columnas siguientes se han ingresado los niveles de las salvaguardas actuales, y objetivo, y la última columna es el nivel que recomienda Pilar recomienda

Como se visualiza en el gráfico, el nivel de salvaguardas actuales está entre 1 a 3, lo cual indica que aún falta definir procesos para mejorar la protección de los activos de información, el objetivo es llegar a medirlos y gestionarlos.

4.4.9. Estimación del Estado de Riesgo

En esta tarea se procesa e interpreta los resultados obtenido de las actividades anteriores para detallar en un informe el estado de riesgo de la Institución. El objetivo es obtener una estimación fundada de lo que puede ocurrir (impacto) y de lo que probablemente ocurra (riesgo).

4.4.9.1. Estimación del Impacto

Con la ayuda de la herramienta Pilar se estimará el impacto potencial y el impacto actual.

El impacto potencial es la medida del daño al que está expuesto todo el sistema de estudio del proyecto, teniendo en cuenta el valor de los activos y la valoración de las amenazas, sin tener en cuenta las salvaguardas actuales.

Gráfico 09: Nivel de impacto
Fuente: Herramienta Pilar 6.2.6

potencial | Actual | Objetivo | PILAR

activo	[D]	[I]	[C]	[A]
ACTIVOS	[10]	[10]	[10]	[10]
[B] Activos esenciales				
[IS] Servicios internos	[10]	[10]	[9]	[10]
[SERV_TEL] Servicio de Telefonía analógica	[10]	[9]	[8]	[10]
[SERV_CORREO] Servicio de Correo Institucional	[10]	[10]	[9]	[10]
[SERV_SOPORTE] Servicio de Soporte técnico	[9]			
[E] Equipamiento	[10]	[10]	[10]	[10]
[SW] Software	[10]	[9]	[9]	[10]
[HW] Equipos	[10]	[10]	[10]	[10]
[COM] Comunicaciones	[9]	[7]	[8]	[10]
[AUX] Elementos auxiliares	[10]			
[SS] Servicios subcontratados	[9]	[6]	[8]	[10]
[INTERNET] Conexión a Internet	[9]	[6]	[8]	[10]
[L] Instalaciones	[10]			
[LOCAL_INF] Área de informática	[10]			
[LOCAL_ADM] Área de Administración	[10]			
[Local_Bal] Área de Balanza	[10]			
[P] Personal	[9]	[9]	[9]	
[JEFE_TI] Encargado del Área de Informática	[9]	[9]	[9]	
[OPER] Operadores en el Área de Balanza	[9]	[8]	[8]	
[USERS] Usuarios Finales	[9]	[8]	[7]	

Gráfico 10: Impacto potencial
Fuente: Herramienta Pilar 6.2.6

El impacto Residual (Actual) es la medida del daño al que está expuesto todo el sistema de estudio del proyecto, teniendo en cuenta el valor de los activos, la valoración de las amenazas y las salvaguardas desplegadas actualmente. Se calcula con los datos del impacto acumulado y las salvaguardas apropiada para cada activo del sistema.

[PDM-ZEDPAITA] impacto y riesgo > impacto acumulado

potencial | Actual | Objetivo | PILAR

activo	[D]	[I]	[C]	[A]
ACTIVOS	[9]	[8]	[8]	[9]
[B] Activos esenciales				
[IS] Servicios internos	[9]	[8]	[7]	[9]
[SERV_TEL] Servicio de Telefonía analógica	[9]	[8]	[6]	[9]
[SERV_CORREO] Servicio de Correo Institucional	[8]	[8]	[7]	[8]
[SERV_SOPORTE] Servicio de Soporte técnico	[8]			
[E] Equipamiento	[9]	[8]	[8]	[9]
[SW] Software	[8]	[7]	[7]	[8]
[HW] Equipos	[9]	[8]	[8]	[9]
[COM] Comunicaciones	[7]	[5]	[6]	[8]
[AUX] Elementos auxiliares	[8]			
[SS] Servicios subcontratados	[7]	[4]	[6]	[8]
[INTERNET] Conexión a Internet	[7]	[4]	[6]	[8]
[L] Instalaciones	[8]			
[LOCAL_INF] Área de informática	[8]			
[LOCAL_ADM] Área de Administración	[8]			
[Local_Bal] Área de Balanza	[8]			
[P] Personal	[8]	[8]	[8]	
[JEFE_TI] Encargado del Área de Informática	[8]	[8]	[8]	
[OPER] Operadores en el Área de Balanza	[8]	[7]	[7]	
[USERS] Usuarios Finales	[8]	[7]	[6]	

Gráfico 11: Impacto residual
Fuente: Herramienta Pilar 6.2.6

4.4.9.2. Estimación de riesgo.

En esta actividad se estima el riesgo al que están sometidos los activos del sistema.

El riesgo potencial, es la medida del daño probable sobre el sistema de estudio, conociendo el impacto de las amenazas sobre los activos, sin tomas en cuenta la existencia de salvaguardas.

Gráfico 12: Niveles de criticidad
Fuente: Herramienta Pilar 6.2.6

[PDM-ZEDPAITA] impacto y riesgo > riesgo acumulado

potencial | Actual | Objetivo | PILAR

activo	[D]	[I]	[C]	[A]
ACTIVOS	{7,2}	{7,2}	{6,8}	{7,7}
[B] Activos esenciales				
[IS] Servicios internos	{6,8}	{6,8}	{6,2}	{6,8}
[SERV_TEL] Servicio de Telefonía analógica	{6,8}	{6,3}	{5,7}	{6,8}
[SERV_CORREO] Servicio de Correo Institucional	{6,8}	{6,8}	{6,2}	{6,8}
[SERV_SOPORTE] Servicio de Soporte técnico	{6,3}			
[E] Equipamiento	{7,2}	{7,2}	{6,8}	{7,7}
[SW] Software	{6,8}	{6,6}	{6,6}	{7,7}
[HW] Equipos	{7,2}	{7,2}	{6,8}	{7,7}
[COM] Comunicaciones	{7,2}	{5,0}	{5,7}	{6,8}
[AUX] Elementos auxiliares	{6,8}	{0}		
[SS] Servicios subcontratados	{7,2}	{4,5}	{5,7}	{6,8}
[INTERNET] Conexión a Internet	{7,2}	{4,5}	{5,7}	{6,8}
[L] Instalaciones	{6,8}			
[LOCAL_INF] Área de informática	{6,8}			
[LOCAL_ADM] Área de Administración	{6,8}			
[Local_Bal] Área de Balanza	{6,8}			
[P] Personal	{6,3}	{6,2}	{6,6}	
[JEFE_TI] Encargado del Área de Informática	{6,3}	{6,2}	{6,6}	
[OPER] Operadores en el Área de Balanza	{6,0}	{5,7}	{6,6}	
[USERS] Usuarios Finales	{6,0}	{5,7}	{5,9}	

Gráfico 13: Riesgo potencial
Fuente: Herramienta Pilar 6.2.6

El riesgo residual (Actual), Dado un conjunto de salvaguardas desplegadas y una medida de madurez de su proceso de gestión, el sistema de estudio ha quedado en una situación de riesgo modificado a un valor residual.

[PDM-ZEDPAITA] impacto y riesgo > riesgo acumulado

potencial | Actual | Objetivo | PILAR

activo	[D]	[I]	[C]	[A]
ACTIVOS	{6,1}	{5,2}	{5,4}	{6,5}
[B] Activos esenciales				
[IS] Servicios internos	{5,5}	{5,0}	{4,1}	{5,5}
[SERV_TEL] Servicio de Telefonía analógica	{5,5}	{5,0}	{4,1}	{5,5}
[SERV_CORREO] Servicio de Correo Institucional	{4,9}	{4,8}	{4,1}	{5,0}
[SERV_SOPORTE] Servicio de Soporte técnico	{5,1}			
[E] Equipamiento	{6,1}	{5,2}	{5,0}	{6,5}
[SW] Software	{5,0}	{4,6}	{4,5}	{5,8}
[HW] Equipos	{6,1}	{5,2}	{5,0}	{6,5}
[COM] Comunicaciones	{5,5}	{2,9}	{4,0}	{5,1}
[AUX] Elementos auxiliares	{5,4}	{0}		
[SS] Servicios subcontratados	{5,4}	{2,7}	{3,9}	{5,1}
[INTERNET] Conexión a Internet	{5,4}	{2,7}	{3,9}	{5,1}
[L] Instalaciones	{5,2}			
[LOCAL_INF] Área de informática	{5,2}			
[LOCAL_ADM] Área de Administración	{5,2}			
[Local_Bal] Área de Balanza	{5,2}			
[P] Personal	{5,1}	{5,1}	{5,4}	
[JEFE_TI] Encargado del Área de Informática	{5,1}	{5,1}	{5,4}	
[OPER] Operadores en el Área de Balanza	{4,9}	{4,6}	{5,4}	
[USERS] Usuarios Finales	{4,9}	{4,6}	{4,7}	

Gráfico 14: Riesgo residual
Fuente: Herramienta Pilar 6.2.6

4.4.10. Interpretación de resultados.

En esta tarea se procesa e interpreta los resultados obtenido de las actividades anteriores para detallar en un informe el estado de riesgo de la Institución. El objetivo es obtener una estimación fundada de lo que puede ocurrir (impacto) y de lo que probablemente ocurra (riesgo).

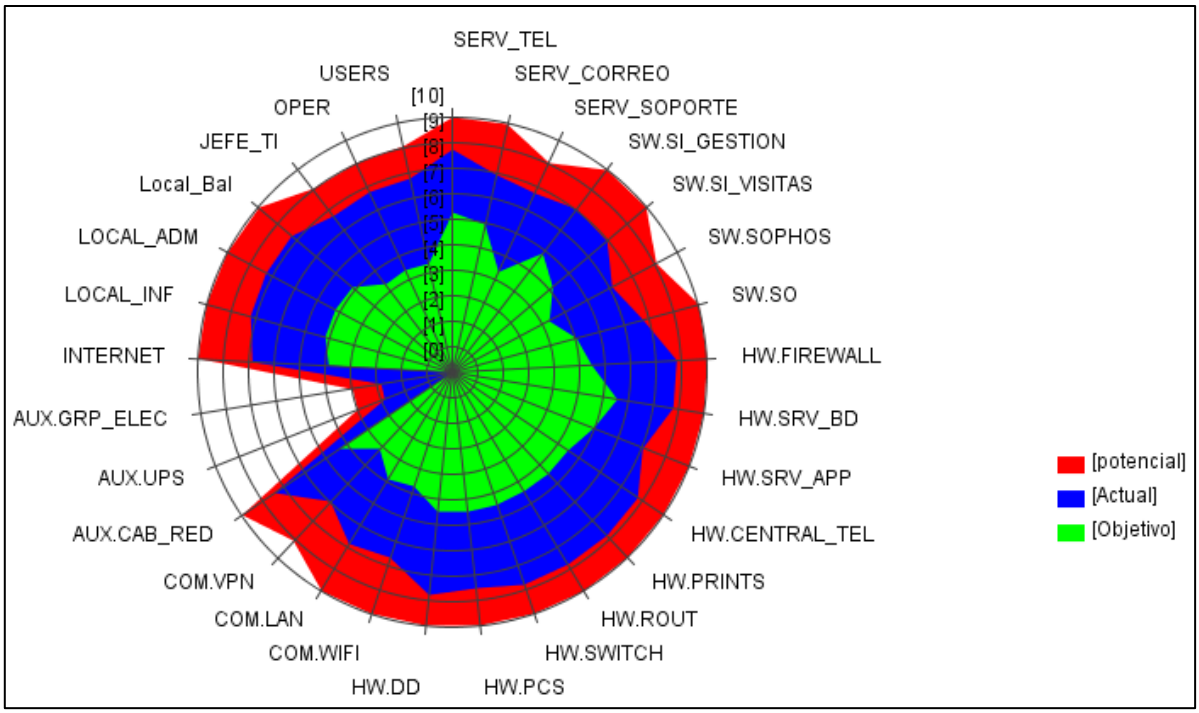


Gráfico 15: Impacto acumulado
Fuente: Herramienta Pilar 6.2.6

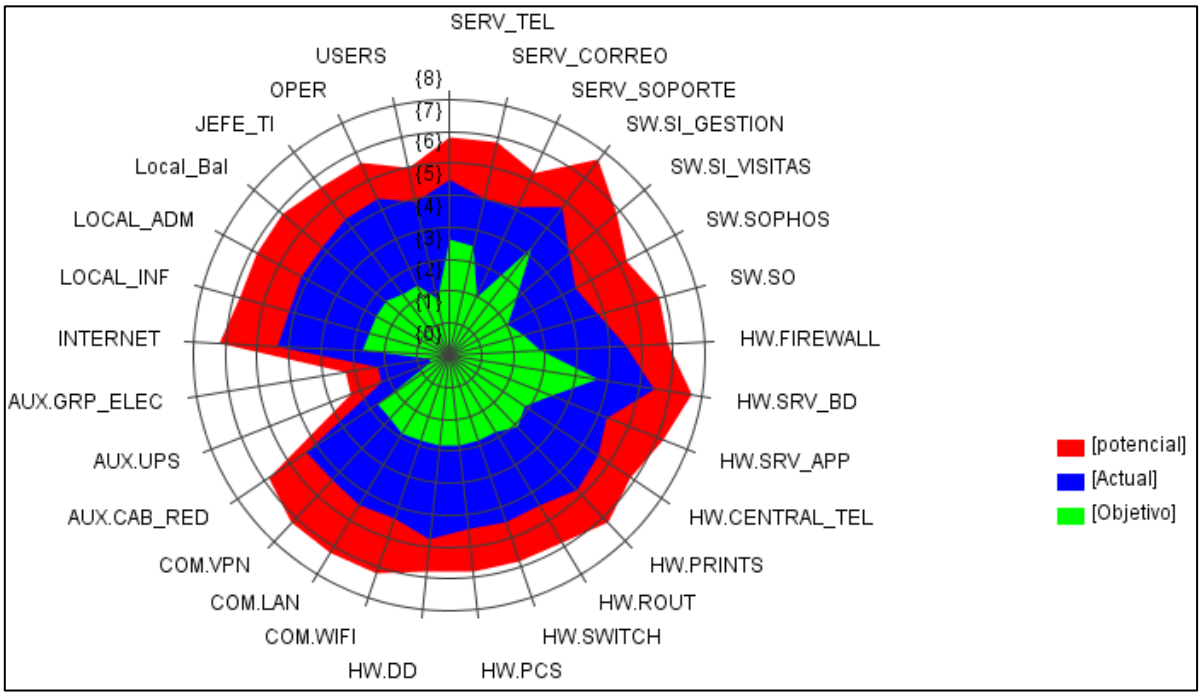


Gráfico 16: Riesgo acumulado
Fuente: Herramienta Pilar 6.2.6

En los gráficos 15 y 16 se reflejan los valores del impacto y riesgos acumulados sobre cada uno de los activos definidos en el proyecto, además se hacen comparaciones de los impactos y riesgos potenciales las cuales se muestran de color rojo, es decir si no existieran salvaguardas en la Institución, se muestran en el color azul, los impactos y riegos residuales o actuales, es decir se puede visualizar el estado actual de la Institución, finalmente con el color verde se muestra el impacto y el riesgo al cual debe de aspirar la Institución, es decir, el nivel recomendado.

4.5. Plan de Mejora.

4.5.1. Introducción.

Para la elaboración del Plan de Mejora, o más conocido como Plan de Seguridad, se tomó como guía referencial la Norma Técnica Peruana – NTP ISO/IEC 27001:2014 – La cual es una adaptación de la norma internacional ISO 27001:2013. Esta norma especifica una serie de requisitos de seguridad de la información a cumplir por la organización para poder implementar, establecer, mantener y mejorar un Sistema de Gestión de Seguridad de la Información.

4.5.2. Responsables.

Gerencia General:

La gerencia debe proporcionar evidencia de su compromiso con el establecimiento, implementación, operación, monitoreo, revisión y mejoramiento del Plan de Mejora. Esta debe asegurar que se cumplan los objetivos propuestos, establecer roles y responsabilidades, comunicar a la Institución la importancia de lograr los objetivos de seguridad de la información, proporcionar los recursos suficientes para desarrollar, revisar y mantener el Plan de Mejora, asegurar que se realicen auditorías internas y realizar revisiones gerenciales del plan.

Comité de Gestión de Seguridad de Información:

Estará conformado por: La administración, Jefatura de asesoría legal y el responsable del área de informática. Este comité será el órgano responsable de que las políticas de seguridad y los procedimientos y prácticas se cumplan y además se las adecuadas con los lineamientos y objetivos de la Institución

Responsables del cumplimiento:

Todos los empleados, terceros y personal a cargo del tercero que interactúan de manera habitual u ocasional accediendo a las instalaciones, locales de proceso de información, información, procesos y recursos tecnológicos de la Institución. Los responsables del cumplimiento deberán informarse del contenido de la presente política, cumplirlo y hacerlo cumplir como parte del desarrollo de sus tareas habituales.

4.5.3. Políticas de Seguridad.

El análisis realizado con la metodología MAGERIT en la identificación y evaluación de riesgos nos facilita el alineamiento con los objetivos y controles de la Norma Técnica Peruana, para el tratamiento adecuado de riesgos, del mismo modo que estos permitirán cumplir con los requisitos legales, reguladores y contractuales. A continuación, se listan los objetivos de control y las acciones recomendadas.

Política de seguridad		
Política de seguridad de información		
Objetivo de control: Proporcionar dirección gerencial y apoyo a la seguridad de la información en concordancia con los requerimientos comerciales y leyes y regulaciones relevantes.		
	Documentar política de seguridad de la información	La gerencia debe aprobar esta política de seguridad, luego se debe publicar y comunicar a todos los empleados y entidades externas relevantes
	Revisión de la política de seguridad de la información	La política de seguridad de la información debe ser revisada regularmente a intervalos planeados o si ocurren cambios significativos

		para asegurar la continua idoneidad, eficiencia y efectividad.
Organización de la seguridad de la información		
Organización interna		
Objetivo: Manejar la seguridad de la información dentro de la organización.		
	Compromiso de la gerencia con la seguridad de la información	La gerencia debe apoyar activamente la seguridad dentro de la organización a través de una dirección clara, compromiso demostrado, asignación explícita y reconocimiento de las responsabilidades de la seguridad de la información.
	Coordinación de la seguridad de información	Las actividades de seguridad de la información deben ser coordinadas por representantes de las diferentes pates de la organización con las funciones y roles laborables relevantes
	Asignación de responsabilidades de la seguridad de la información	Se deben definir claramente las responsabilidades de la seguridad de la información.
	Proceso de autorización para los medios de procesamiento de información	Se debe definir e implementar un proceso de autorización gerencial para los nuevos medios de procesamiento de información
	Acuerdos de confidencialidad	Se deben identificar y revisar regularmente los requerimientos de confidencialidad o los acuerdos de no-divulgación reflejando las necesidades de la organización para la protección de la información.
	Revisión independiente de la seguridad de la información	El enfoque de la organización para manejar la seguridad de la información y su implementación (es decir: objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información) se debe revisar independientes a intervalos planeados, ocurran cambios significativos para la implementación de la seguridad.
Gestión de activos		
Responsabilidad por los activos		
Objetivo: Lograr y mantener la protección apropiada de los activos de la organización		
	Inventarios de activos	Todos los activos deben estar claramente identificados, y se debe elaborar y mantener un inventario de todos los activos importantes.
	Propiedad de los activos	Toda la información y los activos asociados con los medios de procesamiento de la

		información deben de ser “propiedad” de una parte designada de la organización.
	Uso aceptable de los activos	Se deben identificar, documentar e implementar las reglas para el uso aceptable de la información y los activos asociados con los medios de procesamiento de la información.
Clasificación de la información		
Objetivo: Asegurar que la información reciba un nivel de protección apropiado		
	Lineamiento de clasificación	La información debe ser clasificada en términos de su valor, requerimientos legales, confidencialidad y grado crítico para la organización.
	Etiquetado y manejo de la información	Se debe desarrollar e implementar un apropiado conjunto de procedimientos para etiquetar y manejar la información en concordancia con el esquema de clasificación adoptado por la organización.
Seguridad de los recursos humanos.		
Antes del empleo		
Objetivo: Asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades, y sean adecuados para los roles para los cuales se les considera; y reducir el riesgo de robo, fraude o mal uso de los medios.		
	Roles y responsabilidades	Se deben definir y documentar los roles y responsabilidades de seguridad de los empleados, contratistas y terceros en concordancia con la política de la seguridad de información de la organización
	Selección	Se deben llevar a cabo chequeos de verificación de antecedentes de todos los candidatos a empleados, contratistas y terceros en concordancia con las leyes, regulaciones y ética relevante, y deben ser proporcionales a los requerimientos comerciales, la clasificación de la información de la cual se va a tener acceso y los riesgos percibidos.
	Términos y condiciones de empleo	Como parte de su obligación contractual; los empleados, contratistas y terceros deben aceptar y firmar los términos y condiciones de su contrato de empleo, el cual debe establecer sus responsabilidades y las de la organización para la seguridad de la información
Durante el empleo		
Objetivo: Asegurar que todos los empleados, contratistas y terceros estén al tanto de las amenazas e inquietudes sobre la seguridad de información, sus responsabilidades y		

obligaciones, y que estén equipados para apoyar la política de seguridad organizacional en el curso de su trabajo normal, y reducir los riesgos de error humano.		
	Gestión de responsabilidades	La gerencia debe requerir que los empleados apliquen la seguridad en concordancia con las políticas y procedimientos establecidos de la organización
	Capacitación y educación en seguridad de la información	Todos los empleados de la organización deben recibir el apropiado conocimiento, capacitación y actualizaciones regulares de las políticas y procedimientos organizacionales, conforme sean relevantes para su función laboral
	Proceso disciplinario	Debe existir un proceso disciplinario formal para los empleados que han cometido una violación en la seguridad
Terminación o cambio del empleo		
Objetivo: Asegurar que los empleados que salgan de la Institución, lo realicen de manera ordenada, sin violar ninguna regla de seguridad.		
	Devolución de activos	Todos los empleados deben devolver todos los activos de la institución que estén en su poder a la terminación de su contrato.
	Eliminación de derechos de acceso	Los derechos de acceso de los empleados que salen de la organización deben ser eliminados al término de su contrato.
Seguridad física y ambiental		
Áreas seguras.		
Objetivo: Evitar el acceso no autorizado, daño e interferencia a los locales de acceso restringido.		
	Controles de entrada	Se deben proteger las áreas seguras mediante controles de entrada apropiados para asegurar que sólo se permita acceso al personal autorizado.
	Protección contra amenazas externas y ambientales	Se debe diseñar y aplicar protección física contra daño por fuego, inundación, terremoto, explosión, disturbios civiles y otras formas de desastre natural o creado por el hombre
	Área de acceso público, entregas y carga.	Se deben controlar los puntos de acceso, como el área de balanza, donde personas no autorizadas pueden ingresar a los locales, y cuando fuese posible se debe aislar a los medios de procesamiento de la información para evitar un acceso no autorizado.
Seguridad de los equipos informáticos		
Objetivo: Evitar la pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades de la institución		
	Ubicación y protección de los equipos	Los equipos deben estar ubicados en lugares estratégicos y protegidos, para reducir el riesgo de ser extraviados, robados o dañados

		intencionalmente.
	Servicios públicos	Los equipos deben seguir protegidos de las interrupciones eléctricas, a través del grupo electrógeno.
	Seguridad en el cableado	El cableado de la energía y las telecomunicaciones que transportan datos deben ser protegidos de las interceptación o daño
	Mantenimiento de equipos	Los equipos deben ser mantenidos periódicamente, actualizando constantemente para prevenir vulnerabilidades de software.
	Eliminación seguro o re-uso de equipos	Todos los medios de almacenamiento deben ser chequeados para asegurar que se haya removido de manera segura cualquier tipo de datos confidenciales
	Traslado de propiedad	Equipos, información o software no deben ser sacados fuera de la propiedad sin previa autorización
Gestión de las comunicaciones y operaciones		
Procedimientos y responsabilidad operacionales		
Objetivo: Asegurar la operación correcto y segura de los medios de procesamiento de la información		
	Procedimientos de operación documentados	Se deben documentar y mantener los procedimientos de operación de los Sistemas de información, y se deben poner a disposición de todos los usuarios que los necesiten.
	Gestión de cambio de control	Se deben controlar los cambios en los diferentes Sistemas que usa la Institución
	División de deberes	Se deben dividir los deberes y las áreas de responsabilidad para así reducir las oportunidades de una modificación no autorizada o un mal uso de los activos de la Institución
Protección contra software malicioso		
Objetivo: Proteger la integridad del software y la información		
	Controles contra software malicioso	Se deben implementar controles de detección, prevención y recuperación para protegerse de códigos maliciosos y se deben implementar procedimientos de conciencia apropiados.
Respaldo (Back-Up)		
Objetivo: Mantener la integridad y disponibilidad de los servicios de procesamiento de información		
	Respaldo de	Se deben seguir realizando copias de respaldo

	información	de información, además de software esencial, estos deben ser probados regularmente.
Gestión de seguridad de redes.		
Objetivo: Asegurar la protección de la información en redes y la protección de la estructura de soporte		
	Controles de red	Las redes deben ser adecuadamente manejadas y controladas para poder protegerlas de amenazas, incluyendo la información en tránsito
	Seguridad de los servicios de red	Se deben identificar los dispositivos de seguridad, niveles de servicio y los requerimientos e incluirlos en cualquier contrato de servicio de red. Ya sean servicios internos o provisto de terceros
Gestión de medios		
Objetivo: Evitar la divulgación, modificación, eliminación o destrucción no autorizada de los activos de información		
	Gestión de medios removibles	Deben existir procedimientos para la gestión de los medios removibles.
	Eliminación de medios	Los medios deben ser eliminados utilizando procedimientos formales y de una manera segura cuando ya no se les requiera.
	Procedimiento de manejo de la información	Se deben estableces los procedimientos para el manejo y almacenaje de la información para proteger dicha información de una divulgación no autorizada.
	Seguridad de documentación del sistema	Se debe proteger la documentación de un acceso no autorizado.
Monitoreo		
Objetivo: Detectar actividades de procesamiento de información no autorizadas		
	Registro de auditoría	Se deben producir registros de las actividades de auditoría, excepciones y eventos de seguridad de la información y se deben mantener durante un período acordado para ayudar en investigaciones futuras y monitorear el control de acceso.
	Uso del sistema de monitoreo	Deben permanecer los procedimientos para monitorear el uso de los medios de procesamiento de información, pero este resultado de las actividades de monitoreo se debe revisar regularmente.
	Protección de la información del registro	Se deben proteger los medios de registro y la información del registro contra alteraciones y acceso no-autorizado.

	Registros del administrador y operador	Se deben registrar las actividades del administrador y los operadores del sistema.
	Registro de fallas	Las fallas se deben registrar, analizar y se debe tomar la acción apropiada.
	Sincronización de relojes	Los relojes de los sistemas de procesamiento de información, como computadoras y laptops, deben estar sincronizados con una fuente de tiempo exacta acordada.
Control de acceso		
Requerimiento comercial para el control del acceso		
Objetivo: Controlar acceso de información		
	Política de control de acceso	Debe existir un procedimiento formal para la inscripción y des-inscripción para otorgar acceso a todos los sistemas y servicios de información.
	Gestión de privilegios	Debe restringir y controlar la asignación y uso de los privilegios.
	Gestión de la clave de usuario	La asignación de claves se debe controlar a través de un proceso de gestión formal. Generando una clave con más de ocho caracteres, usando mayúsculas, minúsculas , números y caracteres especiales.
	Revisión de los derechos de acceso del usuario	La gerencia debe revisar los derechos de acceso de los usuarios a intervalos regulares utilizando un proceso formal.
Responsabilidades del usuario		
Objetivo: Evitar el acceso de usuarios no autorizados, y el compromiso o robo de la información y los medios de procesamiento de la información.		
	Uso de clave	Se debe requerir que los usuarios sigan buenas prácticas de seguridad en la selección y uso de claves.
	Equipo de usuario desatendido	Se debe requerir que los usuarios se aseguren de dar la protección apropiada al equipo desatendido bloqueando su terminal cuando no se va a estar presente en el área de trabajo.
	Política de pantalla y escritorio limpio	Se debe adoptar una política de escritorio limpio para los documentos y medios de almacenaje removibles y una política de pantalla limpia para los medios de procesamiento de la información.
Control de acceso a redes		
Objetivo: Evitar el acceso no autorizado a los servicios en red		
	Política sobre el uso de servicios de red	Los usuarios sólo deben tener acceso a los servicios para los cuales han sido específicamente autorizados a usar.
	Autenticación del usuario para	Se debe utilizar métodos de autenticación para controlar el acceso de usuarios remotos.

	conexiones externas	
	Identificación del equipo de red	Se debe considerar la autenticación automática del equipo como un medio para autenticar las conexiones desde equipos y ubicaciones específicas.
	Control de conexión de redes	Se debe restringir la capacidad de conexión de los usuarios en las redes compartidas, especialmente aquellas que se extienden a través de los límites organizacionales, en concordancia con la política de control de acceso.
Control de acceso al sistema de operación		
Objetivo: Evitar acceso no autorizado a los sistemas operativos.		
	Identificación y autenticación del usuario	Todos los usuarios deben tener un identificador singular (ID de usuario) para su uso personal y exclusivo, se debe elegir una técnica de autenticación adecuada para verificar la identidad del usuario.
	Sistema de gestión de claves	Los sistemas de manejo de claves deben ser interactivos y deben asegurar la calidad de las claves.
	Uso de utilidades del sistema	Se debe restringir y controlar estrictamente el uso de los programas de utilidad que podrían superar al sistema y controles de aplicación.
	Sesión inactiva	Las sesiones inactivas deben cerrarse después de un período de inactividad definido.
	Limitación de tiempo de conexión	Se debe utilizar las restricciones sobre los tiempos de conexión para proporcionar seguridad adicional a las aplicaciones de alto riesgo.
Control de acceso a la aplicación de la información.		
Objetivo: Evitar el acceso no autorizado a la información mantenida en los sistemas de aplicación.		
	Restricción al acceso a la información	Se debe restringir el acceso de los usuarios y personal de soporte al sistema de información y aplicación en concordancia con la política de control de acceso definida.
	Aislamiento del sistema sensible	Los sistemas sensibles deben tener un ambiente de cómputo dedicado (aislado).
Procesamiento correcto en las aplicaciones		
Objetivo: Evitar errores, pérdida, modificación no-autorizada o mal uso de la información en las aplicaciones		
	Validación de data de consumo	El insumo de data en las aplicaciones debe ser validado para asegurar que esta data es correcta y apropiada.

	Control de procesamiento interno	Se deben incorporar chequeos de validación en las aplicaciones para detectar cualquier corrupción de la información a través de los errores de procesamiento o actos deliberados.
	Integridad del mensaje	Se deben identificar los requerimientos para asegurar la autenticidad y protección de la integridad de mensaje en las aplicaciones, y se deben identificar e implementar los controles apropiados.
	Validación de datos de salida	Se debe validar la salida de datos de una aplicación para asegurar que el procesamiento de la información almacenada sea correcto y apropiado para las circunstancias.
Controles criptográficos		
Objetivo: Proteger la confidencialidad, autenticidad o integridad de la información a través de medios criptográficos).		
	Política sobre el uso de controles criptográficos	Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.
	Gestión clave	Se debe utilizar una gestión clave para dar soporte al uso de las técnicas de la criptografía en la organización.
Seguridad de los archivos del sistema		
Objetivo: Garantizar la seguridad de los archivos del sistema		
	Control de software operacional	Se debe contar con procedimientos para controlar la instalación de software en los sistemas operacionales.
	Protección de la data de prueba del sistema	Se debe seleccionar cuidadosamente, proteger y controlar la data de prueba.
	Control de acceso al código fuente del programa	Se debe restringir el acceso del código fuente del programa.
Gestión de vulnerabilidad técnica		
Objetivo: Reducir los riesgos resultantes de la explotación de vulnerabilidades técnicas publicadas.		
	Control de vulnerabilidades técnicas	Se debe obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas de información en uso; se debe evaluar la exposición de la organización ante esas vulnerabilidades; y se deben tomar las medidas apropiadas para tratar el riesgo asociado.
Gestión de incidentes en la seguridad de la información		
Reporte de eventos y debilidades en la seguridad de la información		
Objetivo: Asegurar que la información de los eventos y debilidades en la seguridad de la información asociados con los sistemas de información sea comunicada de una manera que permita tomar una acción correctiva oportuna.		
	Reporte de los eventos	Los eventos de seguridad de la información

	en la seguridad de la información	deben reportarse a través de los canales gerenciales apropiados lo más rápidamente posible.
	Reporte de las debilidades en la seguridad	Se debe requerir que todos los empleados, contratistas y terceros usuarios de los sistemas y servicios de información tomen nota y reporten cualquier debilidad observada o sospechada en la seguridad de los sistemas o servicios.
Gestión de incidentes y mejoras en la seguridad de la información		
Objetivo: Asegurar que se aplique un enfoque consistente y efectivo a la gestión de la seguridad de la información.		
	Responsabilidades y procedimientos	Se deben establecer las responsabilidades y procedimientos gerenciales para asegurar una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información.
	Aprendizaje de los incidentes en la seguridad de la información	Deben existir mecanismos para permitir cuantificar y monitorear los tipos, volúmenes y costos de los incidentes en la seguridad de la información.
	Recolección de evidencia	Cuando la acción de seguimiento contra una persona u organización después de un incidente en la seguridad de la información involucra una acción legal (sea civil o criminal), se debe recolectar, mantener y presentar evidencia para cumplir las reglas de evidencia establecidas en la(s) jurisdicción(es) relevantes.
Gestión de la continuidad comercial		
Aspectos de la seguridad de la información de la gestión de continuidad comercial		
Objetivo: Contrarrestar las interrupciones de las actividades comerciales y proteger los procesos comerciales críticos de los efectos de fallas o desastres importantes o desastres en los sistemas de información y asegurar la reanudación oportuna.		
	Incluir seguridad de la información en el proceso de gestión de continuidad comercial	Se debe desarrollar y mantener un proceso gerencial para la continuidad del negocio a través de toda la organización para tratar los requerimientos de seguridad de la información necesarios para la continuidad comercial de la organización.
	Continuidad comercial y evaluación de riesgo	Se deben identificar los eventos que causan interrupciones en los procesos comerciales, junto con la probabilidad e impacto de dichas interrupciones y sus consecuencias para la seguridad de la información.

	Desarrollar e implementar planes de continuidad incluyendo seguridad de la información	Se deben desarrollar e implementar planes para mantener o restaurar las operaciones y asegurar la disponibilidad de la información en el nivel requerido y en las escalas de tiempo requeridas después de la interrupción o falla en los procesos comerciales críticos.
	Prueba, mantenimiento y reevaluación de planes de continuidad comercial	Los planes de continuidad comercial se deben probar y actualizar regularmente para asegurar que estén actualizados y sean efectivos.
Cumplimiento con requerimientos legales		
Objetivo: Evitar violaciones de cualquier ley, obligación reguladora o contractual y de cualquier requerimiento de seguridad		
	Identificación de legislación aplicable	Se deben definir explícitamente, documentar y actualizar todos los requerimientos estatuarios, reguladores y contractuales y el enfoque de la organización relevante para cada sistema de información y la organización.
	Derechos de propiedad intelectual (IPR)	Se deben implementar los procedimientos apropiados para asegurar el cumplimiento de los requerimientos legislativos, reguladores y respecto a los derechos de propiedad intelectual y sobre el uso de los productos de software patentados.
	Protección los registros organizacionales	Se deben proteger los registros importantes de una organización de pérdida, destrucción y falsificación, en concordancia con los requerimientos estatuarios, reguladores, contractuales y comerciales.
	Protección de data y privacidad de información personal	Se deben asegurar la protección y privacidad tal como se requiere en la legislación relevante, las regulaciones y, si fuese aplicable, las cláusulas contractuales.
Cumplimiento con las políticas y estándares de seguridad, y el cumplimiento técnico		
Objetivo: Asegurar el cumplimiento de los sistemas con las políticas y estándares de seguridad organizacional		
	Cumplimiento con las políticas y estándar de seguridad	La gerencia deben asegurar que todos los procedimientos de seguridad dentro de su área de responsabilidad sean realizados correctamente en cumplimiento con políticas y estándares de seguridad.
	Chequeo de cumplimiento técnico	Los sistemas de información deben chequearse regularmente para el cumplimiento con los estándares de implementación de la seguridad.
Consideraciones de auditoría de los sistemas de información		
Objetivo: Maximizar la efectividad de y minimizar la interferencia de/desde el proceso de		

auditoría de los sistemas de información		
	Controles de auditoría de sistemas de información	Se deben planear cuidadosamente los requerimientos y actividades de las auditorías que involucran chequeo de los sistemas operacionales y se debe acordar minimizar el riesgo de interrupciones en los procesos comerciales.
	Protecciones de las herramientas de auditoría de los sistemas de información	Se debe proteger el acceso a las herramientas de auditoría de los sistemas de información para evitar cualquier mal uso o compromiso posible.

Tabla 13: Políticas de seguridad
Fuente: Elaborado por el autor, en base a la NTP ISO/IEC 27001:2014

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

CAPITULO V – CONCLUSIONES Y RECOMENDACIONES:

5.1. Conclusiones

- La Institución ZED PAITA cuenta con medidas de seguridad en fase inicial, es decir se ha implementado se acuerdo a los criterios de cada encargado del área de informática. Esto ha conllevado que no se tenga estás medidas guiadas y documentadas y no son adecuadamente aprovechadas.

- El uso de la metodología MAGERIT aportan una gran ayuda para todo el proceso de análisis de los riesgos, desde la identificación de los activos, la valorización de estos, la identificación de las amenazas, conocer las salvaguardas actuales y nos ayudan con la implementación de las futuras salvaguardas para controlar y mitigar los riesgos encontrados.

- El uso de la Herramienta PILAR fue de gran ayuda para conocer los riesgos e impactos a los que está expuesto todo el sistema, a través de los resultados se puede conocer el impacto que generaría la materialización de las amenazas, además sus gráficas comparan los impactos actuales, y misma herramienta nos propone un impacto recomendado basados en estándares internacionales de gestión de la seguridad de la información.

- Una vez realizado todo el estudio siguiendo la metodología, se pudo elaborar una propuesta de Plan de Mejora de la seguridad de la información, este plan fue elaborado en el marco del cumplimiento de la NTP ISO/IEC 27001:2014, la cual es obligatoria en todas las instituciones del estado.

5.2. Recomendaciones

- La Institución debe de realizar el proceso de verificación y actualización de los riesgos y amenazas de los que constantemente estas expuestos sus activos, esto debido a que el cambio tecnológico es constante y cada vez se descubren nuevas formas de vulnerar las diferentes salvaguardas implementadas.

- Se recomienda implementar el Plan de Mejora propuesto, el cual puede ser modificado, actualizado o interpretado de la mejor forma posible, de tal manera que se reduzca el impacto generado por la materialización de alguna amenaza.

- Se debe capacitar a los usuarios para el correcto desarrollo de las actividades, minimizando los riesgos, comprendiendo la importancia de su colaboración en el esfuerzo de mantener el entorno seguro.

- Se debe dejar constancia de que los usuarios fueron informados respecto a las políticas que implementa la Institución, y de su completa comprensión y su conformidad respecto a su cumplimiento.

- Se debe implementar una base de datos de todos los activos con los que cuenta la institución, la cual debe ser actualizada constantemente.

- El presente proyecto puede ser usado como base para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), ya que cumple con la parte básica para la implementación del mencionado sistema, que es en análisis actual de la Institución.

BIBLIOGRAFÍA:

Afore, c. (08 de Setiembre de 2016). Obtenido de Administración del Riesgo: http://www.aforecoppel.com/index.php?opcion=33

Congreso del Perú, P. (2013). *Ley de Delitos Informáticos*. Obtenido de Sitio Web del Congreso del Perú: http://www.leyes.congreso.gob.pe/Documentos/Leyes/30096.pdf

Departamento de Seguridad Informática, U. N. (08 de Setiembre de 2016). Obtenido de Seguridad Informática: http://www.seguridadinformatica.unlu.edu.ar/?q=node/12

Did, P. (08 de Setiembre de 2016). *La Tecnología Virtual*. Obtenido de http://latecnologiavirtual.blogspot.pe/2009/06/sistemas-y-tratamiento-de-la.html

ELMARSI, R. y. (s.f.). *Sistemas de Bases de Datos.* Addison- Wesley Iberoamericana.

Gaona, K. (2013). *Aplicación De La Metodología Magerit Para El Análisis Y Gestión De Riesgos En Los Servidores De Los Sistemas De Gestión Académica De La Universidad Nacional Pedro Ruiz Gallo.* Cuenca - Ecuador.

García, A. (2016). *Implementación de un Sistema de Gestión de Seguridad de la Información, Aplicado a los riesgos asociados a los activos de información en la empresa NET - Consultores S.A.C.* Tarapoto - Perú.

Guevara, J. (2015). *Aplicación De La Metodología Magerit Para El Análisis Y Gestión De Riesgos En Los Servidores De Los Sistemas De Gestión Académica De La Universidad Nacional Pedro Ruiz Gallo.* Lambayeque - Perú.

Hernandez, R. (2009). *Auditoría Informática: Un Enfoque Metológico y Práctico.* México: Continental.

INDECOPI, P. (2014). *Norma Técnica Peruana*. Obtenido de Sitio Web de PeCert (Coordinadora de Respuestas a Emergencias en Redes Teleinformáticas de la Administración Pública del Perú): http://www.pecert.gob.pe/_publicaciones/2014/ISO-IEC-27001-2014.pdf

ISO 2700, I. (2013). *ISO 2700. Sistema de gestión de seguridad de la información. Términos de uso información.*

Izquierdo, F. (2005). *Administración de riesgos de tecnología de información de una empresa del sector informático.* Guayaquil - Ecuador.

MARQUEZ, M. (Agosto del 2009). *Clasificación de los Sistemas de Gestión de Bases de Datos.*

Muñoz, C. (2002). *Auditoría en Sistemas Computacionales.* Pearson.

PCM. (06 de Setiembre de 2016). *Ley de Protección de Datos Personales*. Obtenido de Presidencia de Consejo de Ministros: http://www.pcm.gob.pe/transparencia/Resol_ministeriales/2011/ley-29733.pdf

Perafán, J. J., & Caicedo, M. (2014). *Análisis de Riesgos de la Seguridad de la Información para la Institución Universitaria Colegio Mayor Del Cauca.* Popayán - Colombia.

Piattini, M. (2001). *Auditoría Informática: Un Enfoque Práctico.* Madrid - España: RA-MA.

Pinilla, J. (1997). *Auditoría Informática - Aplicaciones en Producción: Análisis de riesgos.* Santa Fe de Bogotá: ECOE.

Rivas, G. A. (1988). *Auditoría Informática.* Madrid: Diaz de Santos, S.A. Obtenido de http://www.dharma.es/index.php/auditoriainformatica/auditoria-informatica

Ruiz, H. (2008). *Política de Seguridad de la Información de la Superintendencia de Sociedades.*

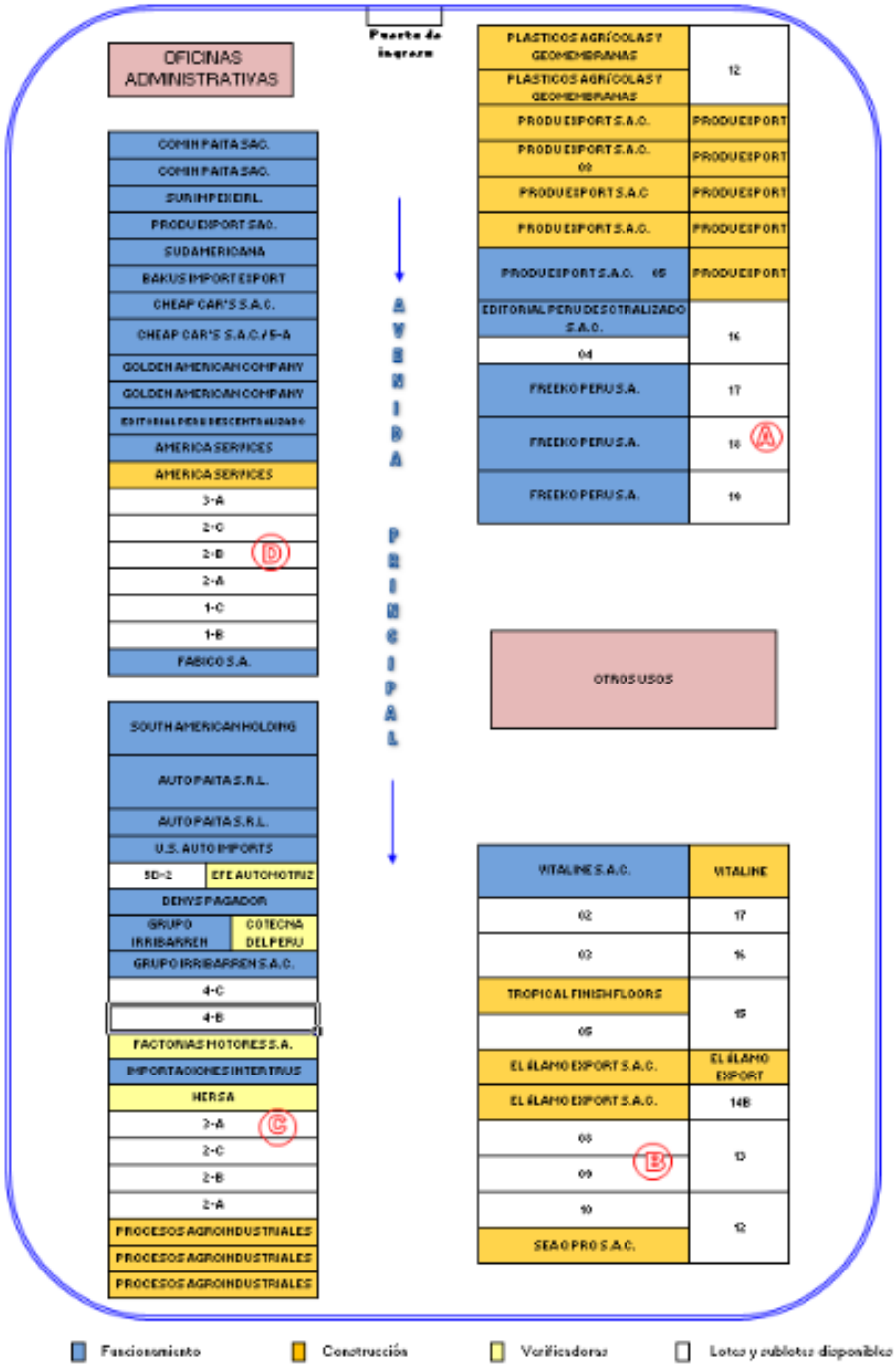
SeguridadPC.Net, S. (08 de Setiembre de 2016). *Conceptos: Seguridad PC*. Obtenido de Seguridad pc: http://www.seguridadpc.net/conceptos.htm

SILBERSCHATZ, K. S. (2002). *Fundamentos de Bases de Datos.* Madrid: Mc- Graw Hill.

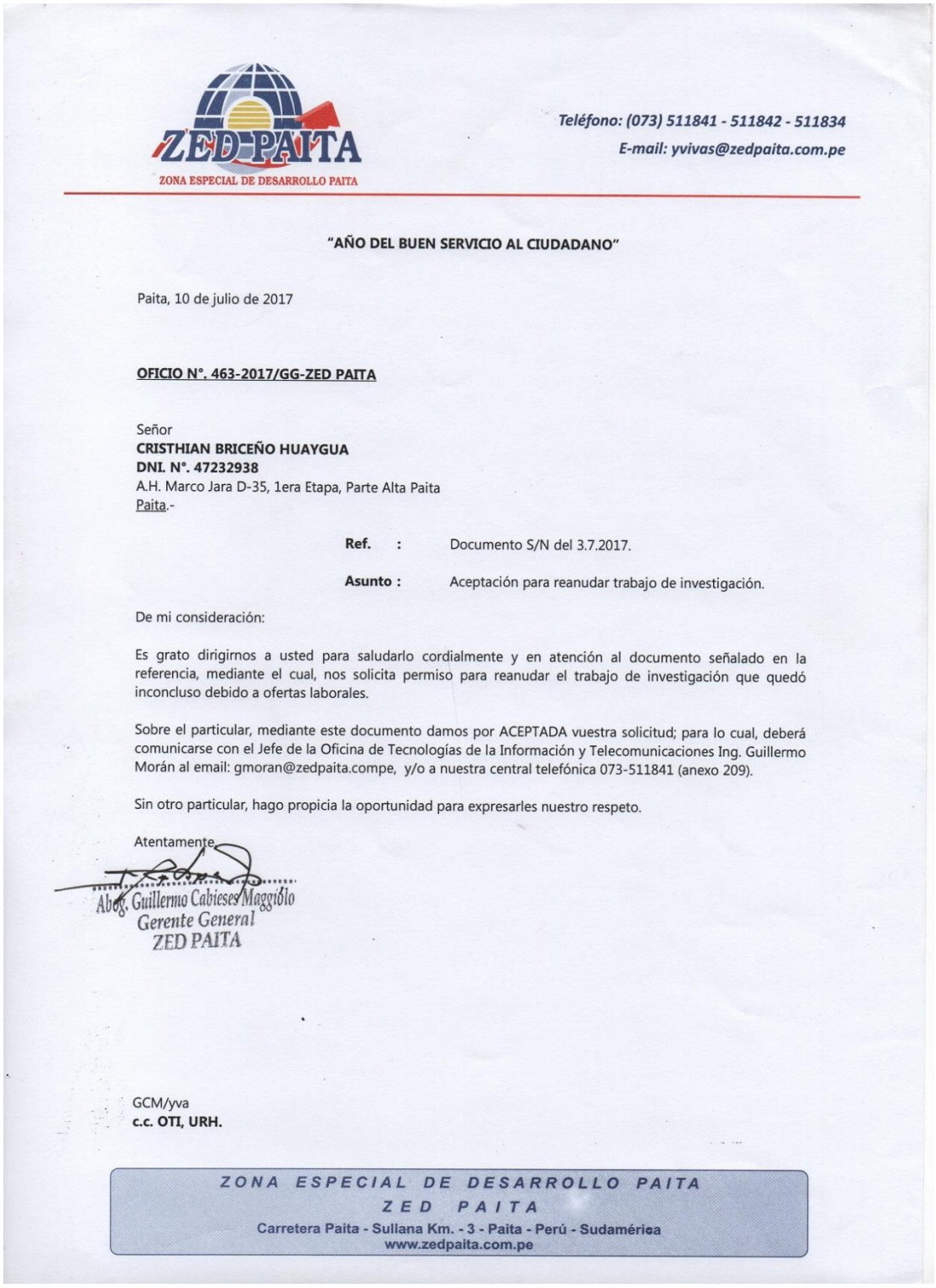
Yangua, B. E. (2014). *Auditoría Informática y su Incidencia en los Riesgos para el Manejo de la Información en la Cooperativa de Ahorro y Crédito Educadores de Tungurahua.* Ambato - Ecuador.

ANEXOS

A. Plano de la Institución ZED - PAITA



B. Aceptación de la Institución para realizar el proyecto.



ZED PAITA
ZONA ESPECIAL DE DESARROLLO PAITA

Teléfono: (073) 511841 - 511842 - 511834
E-mail: yvivas@zedpaita.com.pe

"AÑO DEL BUEN SERVICIO AL CIUDADANO"

Paita, 10 de julio de 2017

OFICIO N°. 463-2017/GG-ZED PAITA

Señor
CRISTHIAN BRICEÑO HUAYGUA
DNI. N°. 47232938
A.H. Marco Jara D-35, 1era Etapa, Parte Alta Paita
Paita.-

Ref. : Documento S/N del 3.7.2017.

Asunto : Aceptación para reanudar trabajo de investigación.

De mi consideración:

Es grato dirigirnos a usted para saludarlo cordialmente y en atención al documento señalado en la referencia, mediante el cual, nos solicita permiso para reanudar el trabajo de investigación que quedó inconcluso debido a ofertas laborales.

Sobre el particular, mediante este documento damos por ACEPTADA vuestra solicitud; para lo cual, deberá comunicarse con el Jefe de la Oficina de Tecnologías de la Información y Telecomunicaciones Ing. Guillermo Morán al email: gmoran@zedpaita.compe, y/o a nuestra central telefónica 073-511841 (anexo 209).

Sin otro particular, hago propicia la oportunidad para expresarles nuestro respeto.

Atentamente,

Abog. Guillermo Cabieses Maggiolo
Gerente General
ZED PAITA

GCM/yva
c.c. OTI, URH.

ZONA ESPECIAL DE DESARROLLO PAITA
ZED PAITA
Carretera Paita - Sullana Km. - 3 - Paita - Perú - Sudamérica
www.zedpaita.com.pe

C. Fichas de recojo de información

[service] Servicio	
código:	**nombre:**
descripción:	
responsable:	
tipo (marque todos los adjetivos que procedan) Ver Sección 2.1.	

Valoración de los servicios que ofrece la Organización a otros, típicamente en las siguientes dimensiones:

[D] disponibilidad

[A] autenticidad de quién accede al servicio

[T] trazabilidad de quién accede al servicio, cuándo y que hace

Valoración		
dimensión	***valor***	***justificación***
[D]		
[A]		
[T]		

[D] Datos / Información	
código:	**nombre:**
descripción:	
responsable:	
tipo (marque todos los adjetivos que procedan) Ver Sección 2.3.	

Las dependencias normalmente identifican

- equipos que los hospedan
- líneas de comunicación por las que se transfieren
- soportes de información
- personas relacionadas: usuarios.

Dependencias de activos inferiores (hijos)	
activo:	**grado:**
¿por qué?:	

activo:	**grado:**
¿por qué?:	

activo:	**grado:**
¿por qué?:	

[SW] Aplicaciones (software)	
código:	**nombre:**
descripción:	
responsable:	
tipo (marque todos los adjetivos que procedan) Ver Sección 2.6.	

Las dependencias normalmente identifican

- personas relacionadas con esta aplicación: operadores, administradores y desarrolladores.

Dependencias de activos inferiores (hijos)	
activo:	**grado:**
¿por qué?:	

[HW] Equipamiento informático (hardware)	
código:	**nombre:**
descripción:	
responsable:	
ubicación:	
número:	
tipo (marque todos los adjetivos que procedan) Ver Sección 2.7.	

Las dependencias normalmente identifican

- personas relacionadas con este equipo: operadores, administradores
- instalaciones que lo acogen

Dependencias de activos inferiores (hijos)	
activo:	**grado:**
¿por qué?:	
activo:	**grado:**
¿por qué?:	

[AUX] Equipamiento auxiliar	
código:	**nombre:**
descripción:	
responsable:	
ubicación:	
número:	
tipo (marque todos los adjetivos que procedan) Ver Sección 2.10.	

Las dependencias normalmente identifican

- personas relacionadas con este equipo: operadores, administradores

Dependencias de activos inferiores (hijos)	
activo:	**grado:**
¿por qué?:	

[L] Instalaciones	
código:	**nombre:**
descripción:	
responsable:	
ubicación:	
número:	
tipo (marque todos los adjetivos que procedan) Ver Sección 2.11.	

Las dependencias normalmente identifican

- personas relacionadas con esta instalación: guardias, encargados de mantenimiento

Dependencias de activos inferiores (hijos)	
activo:	**grado:**
¿por qué?:	
activo:	**grado:**
¿por qué?:	